НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»

Завідувач кафедри

_____ Л.О. Уривський

«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.050903 Телекомунікації
(172 Телекомунікації та радіотехніка)

на тему: «Аналіз принципів побудови сервісу VPN»

Виконав:

студент IV курсу, групи ТС-51

Дьомін Роман Валерійович _____

Керівник:

Доцент, кандидат технічних наук, доцент,

Созонник Г.Д. _____

Рецензент:

Доцент, кандидат технічних наук, доцент,

Варфоломеєва О.Г. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ – 2019 року

РЕФЕРАТ

Текстова частина дипломної роботи: 76 с., 21 рис., 12 джерел, 5 плакатів.

Мета роботи - огляд сучасних технологій щодо надання сервісу побудови віртуальних приватних мереж, аналіз технічних рішень технології VPN на прикладі організації приватної віртуальної мережі на основі мережі MPLS.

В дипломній роботі проведено аналіз та порівняння існуючих підходів побудови віртуальних приватних мереж. Розглядається принцип формування та класифікація VPN, основні концепції організації віртуальної приватної мережі. Розроблені критерії порівняння та здійснено аналіз та порівняння по розробленим критеріям розглянутих технологій. Приведено приклад організації сервісу VPN для корпоративних клієнтів.

ABSTRACT

Text part of the thesis: 76 p., 21 figures, 12 sources, 5 posters.

The purpose of the work is to provide an overview of modern technologies for the provision of virtual private network services, analysis of technical solutions for VPN technology, for example, for the organization of a private virtual network based on the MPLS network.

In a thesis work the analysis and comparison of existing approaches of construction of virtual private networks is carried out. The principle of formation and classification of VPN, the basic concepts of organization of virtual private network is considered. The criteria of comparison have been developed and the analysis and comparison on the developed criteria of the considered technologies has been carried out. An example of a VPN service for corporate clients is provided.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN - (Virtual Private Network) – віртуальна приватна мережа.

MPLS – (Multiprotocol Label Switching) – багатопротокольна комутація по міткам.

NGN – (Next Generation Network) – мережі нового покоління.

IP – (Internet Protocol) – міжмережевий протокол.

BGP – (Border Gateway Protocol) – протокол граничного шлюзу.

VR – (Virtual Reality) – віртуальна реальність.

VPLS – (Virtual Private Local Area Network Service) – віртуальна приватна локальна мережа).

WAN – (Wide Area Network) – глобальна мережа.

Frame Relay – ретрансляція кадрів.

ATM – (Asynchronous Transfer Mode) – асинхронний спосіб передачі даних.

L2 VPN – Layer 2 VPN.

L3 VPN – Layer 3 VPN.

POP – (Point of precense) – точка присутності.

ПК – персональний комп’ютер.

ПЗ – програмне забезпечення.

PPTP – (Point-to-Point Tunneling Protocol) – тунельний протокол точка-точка.

PPPoE – (Point-to-point protocol over Ethernet) – протокол передачі кадрів PPP через Ethernet.

IPSec – (IP Security) – протокол захисту даних , що передається через IP.

ЛОМ – локальна обчислювальна мережа.

TCP – (Transmission Control Protocol) – протокол керування передачею даних.

CER – (Customer Enge Router) – граничний маршрутизатор клієнта.

PER – (Provider Enge Router) – граничний маршрутизатор мережі провайдера.

MAC – (Media Access Control) – фізична адеса пристрою.

LSP – (Label Switch Path) – тунель, шлях в MPLS.

EIGRP – (Enhanced Interior Gateway Routing Protocol) – протокол маршрутизації.

OSPF – (Open Shortest Path First) – протокол динамічної маршрутизації.

VRF – (Virtual Routing and Forwarding) – технологія, що дозволяє реалізовувати на базі одного фізичного маршрутизатора мати декілька віртуальних.

CEF – (Cisco Express Forwarding) – технологія високошвидкісної маршрутизації.

STP – (Spanning Tree Protocol) – протокол покривного дерева.

VLAN – (Virtual Local Area Network) – віртуальна локальна мережа.

LAN – (Local Area Network) – локальна мережа.

LSR – (Label switching router) — комутуюхий мітки маршрутизатор.

ВСТУП

Сучасне суспільство характеризується проникненням бізнесу у всі сфери людського життя. При цьому в діловому світі можна спостерігати дві незаперечні тенденції - до укрупнення бізнесу і до все більшої ролі, яку в ньому грають сучасні системи комунікації.

Дійсно, керування великою компанією може бути успішним лише в разі узгодженості дій її структурних підрозділів. Крім того, треба пам'ятати, що глобальна мережа Інтернет давно вже перестала бути тільки мережею передачі даних і навіть її цінність, як криниці інформації, з точки зору ділового співтовариства, також відходить на задній план. Інтернет сьогодні - це одночасно і активний споживчий ринок, і товарна і валютна біржа: щодня в мережі відбуваються угоди на астрономічні суми. Але сучасні послуги зв'язку необхідні не тільки діловим замовникам - зв'язок все частіше використовується рядовими користувачами: вона стає доступом до популярних розваг, елементом престижу, засобом заробітку і т.д. По мірі розвитку і ускладнення послуг зв'язку, вони ,зазвичай, стають більш вимогливі до ресурсів мережі зв'язку, на базі якої вони надаються. Внаслідок цього термін «сучасні послуги зв'язку» часто нероздільний з поняттям «широкосмугові послуги зв'язку».

Попит на такі послуги призвів до революційної зміни сучасних телекомунікаційних мереж і завданням будь-якого оператора і провайдера послуг стає знаходження оптимального способу їх надання з найбільшою вигодою для себе і з найкращою якістю для замовника. Однією з технологій, що сприяли згаданої революції є технологія MPLS. Незважаючи на свій досить молодий вік, вона стала вже дуже популярною і їй навіть пророкують місце технології 6 передачі даних в т.зв. мережах наступного покоління NGN. Успіх технології MPLS викликаний тим, що вона дозволяє ефективно управляти мережами, збудованими на базі

найбільш значимого і поширеного протоколу - IP. Ця технологія зараз впроваджується в мережах багатьох світових компаній, а в високорозвинених країнах починає домінувати в мережах передачі даних.

Саме це послужило спонукальним моментом вибору теми дипломної роботи - розглянути можливість надання широкосмугових послуг зв'язку на базі технології MPLS.

Надання широкосмугових послуг можна умовно поділити на дві окремі завдання: організація широкосмугового доступу і організація такої інфраструктури опорної мережі оператора, що дозволить здійснювати трансляцію широкосмугового трафіку в мережу доступу. MPLS - технологія магістральних мереж, тому що наводяться в даній роботі дослідження будуть присвячені тільки другий із зазначених завдань. Основною мережевою структурою для надання широкосмугових послуг в магістральній мережі давно стали різноманітні віртуальні мережі, які дозволяють розділити користувачів вузькосмугових і широкосмугових послуг, керувати якістю при наданні широкосмугових послуг і оптимізувати використання ресурсів мережі. В рамках технології MPLS, на даний момент існує три варианти організації віртуальных мереж- це BGP-MPLS VPN, VR VPN і VPLS. Перші два підходи відносять до класу VPN, що організовуються на третьому рівні моделі OSI, а останній – до класу VPN, що організовуються на другому рівні. Низька поширеність і прогнозована відсутність перспектив у підходу VR VPN дозволяє обмежити дослідження тільки двома підходами.

Віртуалізація канальних ресурсів територіально розподілених мереж (WAN) почалася дуже давно, з появою технологій Frame Relay і ATM. Вони дозволяли надавати корпоративним користувачам аналог приватної мережі (виділений ресурс) на основі мережі загального користування оператора зв'язку (розподіляємий ресурс), у чому, власне кажучи, і полягає суть побудови віртуальних приватних мереж (VPN). Однак сьогодні Frame

Relay і ATM відійшли в минуле, а в світі розподілених мереж переважають Ethernet і IP. Сучасні технології VPN дозволяють незалежно від відстані між вузлами емулювати комутатор Ethernet (L2 VPN) або маршрутизації IP-мережу (L3 VPN).

Стрімке зростання ринку послуг VPN почалося з появою технології MPLS.

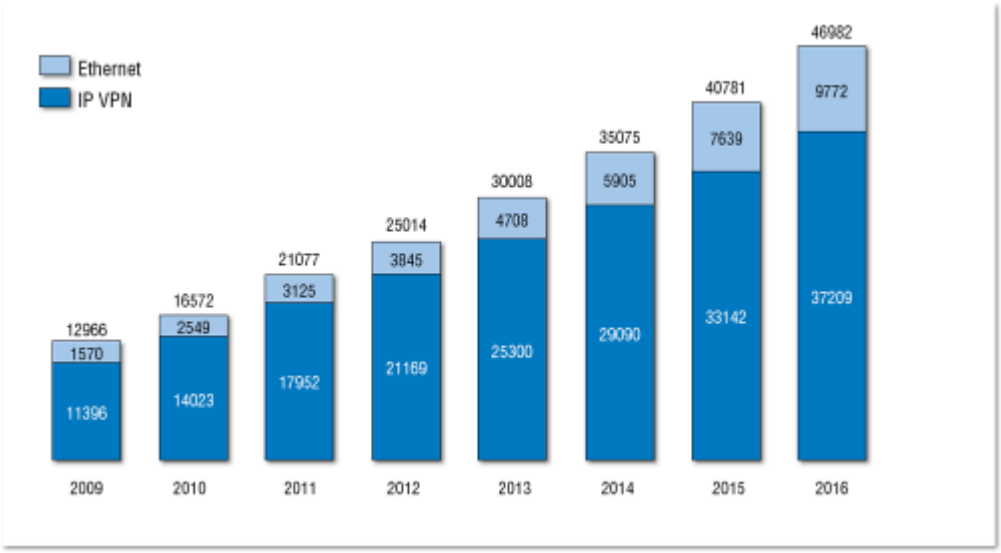


Рисунок 1 Об’єм ринку послуг Ethernet та IP VPN в 2009–2011 роках і прогноз до 2016 року

Активне зростання ринку VPN почалося в 2012-2013 році. Основні фактори, які призвели до зростання попиту на послуги сервісів VPN є: зростання рівня кіберзагроз, геополітичні конфлікти, які призводять до блокування ресурсів для користувачів деяких країн і високий рівень цензури. Так само важливим фактором, що сприяв зростанню користувачів сервісів VPN в світі, стало стрімке зростання користувачів Інтернету в усіх країнах світу. Кількість користувачів мережі Інтернет налічує близько 4 млрд. Чоловік по всьому світу. Щодня сервісами VPN в світі користуються близько 250-280 млн. Чоловік. Найбільший попит на

дані сервіси спостерігається серед користувачів з країн Азіатсько-Тихоокеанського регіону.

Найбільше розповсюдження VPN-сервіси отримали в країнах Азії, Близького Сходу та Латинської Америки.

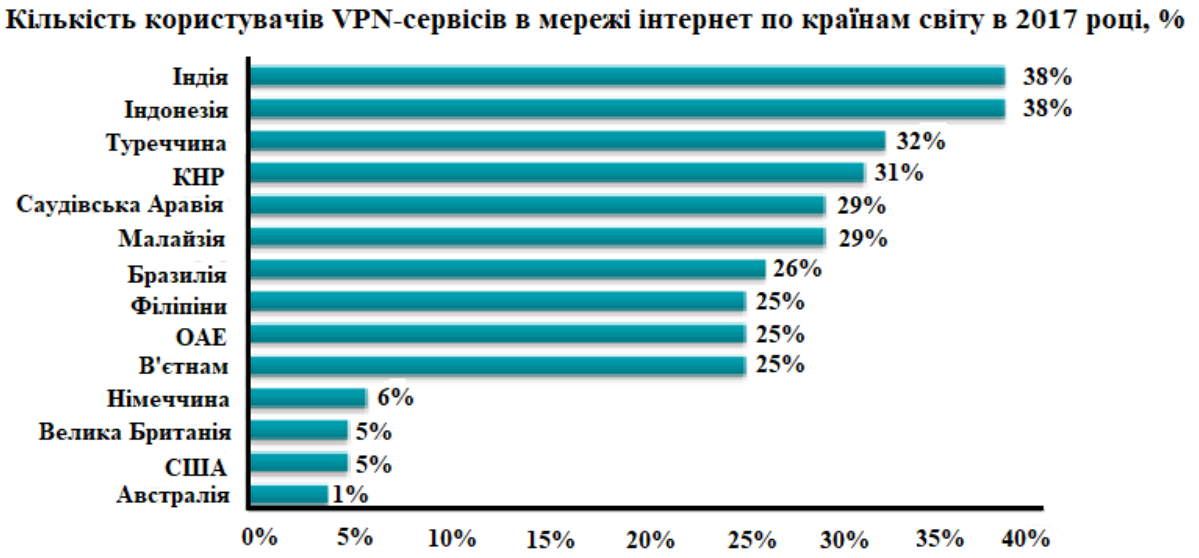


Рисунок 2 Країни, де використовується VPN найбільше

Підвищується інтерес до VPN і з боку пересічних громадян. Особливо в тих країнах, де широко застосовується цензура інтернету і забороняють доступ до популярних ресурсів. Організація VPN-каналів через сервери інших юрисдикцій дозволяє обійти такі заборони. У державному та корпоративному секторах VPN частіше використовується для віддаленого доступу до робочої інформації.

Рисунок 3 Цілі використання VPN

В структурі використання VPN за типами пристроїв тримає лідерство ПК, проте за останній час найбільший приріст показав сегмент мобільних телефонів.

У 2018 році обсяг ринку програмного забезпечення для організації VPN і відповідних послуг оцінювався в $ 12-20 млрд з прогнозом щорічного зростання в 12-15%. Лідерами по вкладенню коштів в VPN є банківські та фінансові організації (сектор BFSI). У цьому секторі ринок VPN виріс в 2017 році на 21,5%.

В останні роки, коли все більша кількість компаній для забезпечення зв'язку почали використовувати глобальну мережу Internet, ринок віртуальних приватних мереж (VirtualPrivateNetwork – VPN) значно збільшився та розширився. В період з 2011 по 2016 роки середній темп зростання ринку послуг L2 VPN склав 26%, а послуг IP VPN — 16% (див. Рисунок). За даними Infonetics Research вартість ринку VPN збільшується близько 10% на рік, що показує його актуальність у світі та в Україні зокрема. Очікується, що до 2019 року ринок VPN набере близько 90 млрд. доларів.

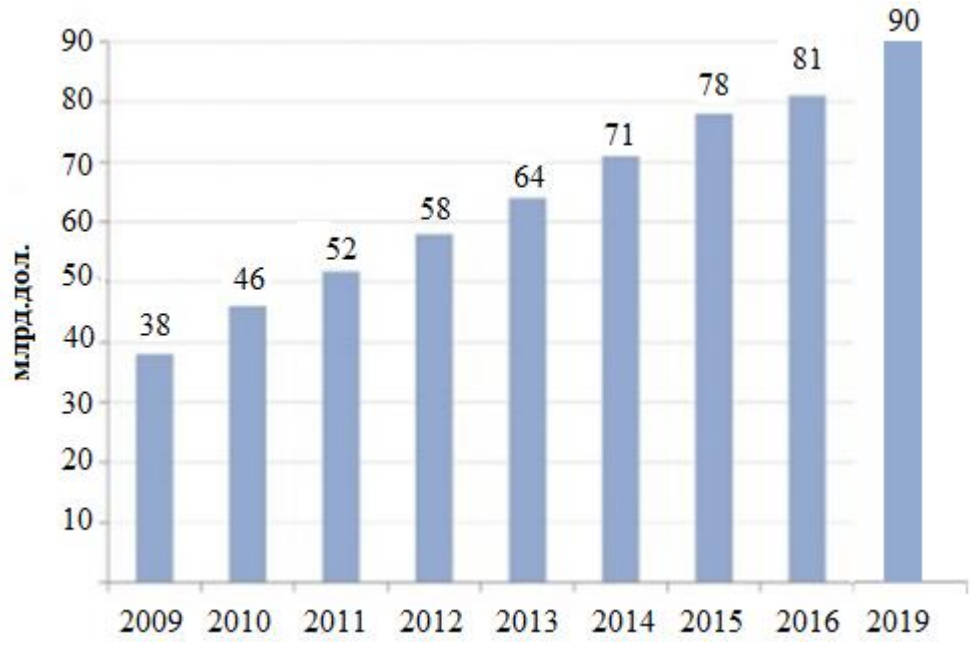


Рисунок 4 Збільшення вартості ринку VPN з роками

Таким чином, ринок VPN неухильно зростав досі, та має тенденцію до зростання. Саме тому, все більше інтернет провайдерів пропонують дану послугу, що вказує, на її актуальність у наш час і зростання інтересу до неї у найближчий період.

1 ЗАГАЛЬНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ VPN

1.1 Основи VPN

VPN (Virtual Private Network) — це віртуальна приватна мережа або логічна мережа, яка створюється поверх незахищених мереж (мереж оператора зв’язку або сервіс-провайдера Інтернет). VPN – це технологія, яка забезпечує захист даних при передачі їх по незахищеним мережам.

Віртуальна мережа - це виділена мережа на базі загальнодоступної мережі, що підтримує конфіденційність інформації, що передається за рахунок використання тунелювання та інших процедур захисту.

В основі технології VPN лежить ідея забезпечення доступу віддалених користувачів до корпоративних мереж, які містять конфіденційну інформацію через мережі загального користування. Як середовище для створення VPN можуть виступати мережі Frame Relay, ATM, але найбільш популярні технології VPN, розраховані на створення мереж VPN в середовищі Інтернет.

Без сумніву, використання каналів Інтернет для організації VPN дозволяє вигідно вирішити проблему організації мережі. Правда, через її загальнодоступність виникає проблема безпеки, адже до ресурсів Інтернет може отримати доступ будь-яка людина.

Віртуальні приватні мережі можуть гарантувати, що направлений через Інтернет трафік, так само захищений, як і при передачі всередині локальної мережі, при збереженні всіх фінансових переваг, які можна отримати, використовуючи Інтернет.

Безпека даних технологією VPN забезпечується за рахунок застосування спеціальних пристроїв і механізмів захисту. Для отримання доступу до мережі користувач VPN проходить через брандмауер, де здійснюється його аутентифікація і авторизація, завдяки чому VPN гарантує, що доступ до ресурсів мережі отримають лише авторизовані користувачі.

Крім того, для передачі VPN-трафіку в мережі загального користування застосовуються механізми тунелювання і шифрування. Це дозволяє зробити приватну інформацію невидимою для інших користувачів Web і забезпечує додатковий захист при передачі.

За своєю суттю, VPN володіє багатьма властивостями виділеної лінії, проте реалізується вона в межах загальнодоступного середовища Інтернет.

Проводячи порівняння між приватними і віртуальними приватними мережами, слід виділити ряд безсумнівних переваг VPN:

- технологія VPN дозволяє значно знизити витрати для утримання працездатності мережі: користувач сплачує тільки абонентську плату за оренду каналу. До речі, оренда каналів також не викликає будь-яких труднощів внаслідок широкомасштабності мережі Інтернет.

- зручність і легкість при організації та перебудови структури мережі;

Розробка єдиної моделі обслуговування віртуальної приватної мережі могла б спростити мережеві операції, але такий підхід не може задовольнити різним вимогам клієнтів, так як вони унікальні. Кожен клієнт висуває свої вимоги до безпеки, числу сайтів, складності маршрутизації, критичних ситуацій, моделям і обсягами трафіку. Для задоволення широкого спектру вимог, постачальники послуг повинні пропонувати клієнтам різні моделі доставки послуг.

Всі мережі VPN умовно можно розділити на три основні види:

- Внутрішнькорпоративні VPN (Intranet VPN).
- Міжкорпоративні VPN (Extranet VPN).
- VPN з віддаленим доступом (Remote Access VPN).

Intranet VPN являє собою найбільш простий варіант VPN, він дозволяє об'єднати в єдину захищену мережу кілька розподілених філій однієї організації, взаємодіючих по відкритих каналах зв'язку.

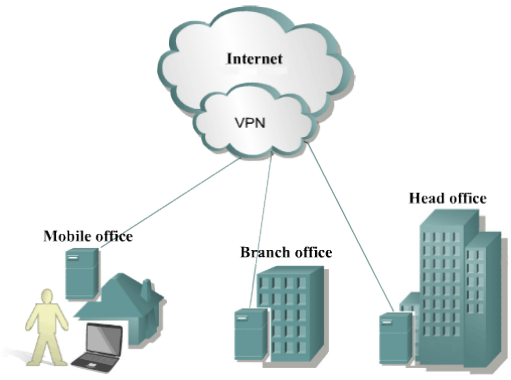


Рисунок 1.1 Приклад мережі Intranet VPN

При організації такої схеми підключення необхідна наявність VPN серверів, яке дорівнює кількості пов'язаних офісів.

Варіант побудови Extranet VPN призначений для забезпечення доступу з мережі однієї компанії до ресурсів мережі іншого, рівень довіри до якої набагато нижче, ніж до своїх співробітників. Тому, коли кілька компаній приймають рішення працювати разом і відкривають один для одного свої мережі, вони повинні подбати про те, щоб їх нові партнери мали доступ тільки до певної інформації. При цьому, конфіденційна інформація повинна бути надійно захищена від несанкціонованого використання. Саме тому в міжкорпоративних мережах велике значення має надаватися контролю доступу за допомогою брандмауерів (Firewalling). Важлива і аутентифікація користувачів, яка покликана гарантувати, що доступ до інформації отримують тільки ті, кому він дійсно дозволений.

Принцип роботи VPN з віддаленим доступом простий: користувачі встановлюють з'єднання з місцевої точкою доступу до глобальної мережі (POP), після чого їх виклики тунелюють через Інтернет, що дозволяє уникнути плати за міжміський і міжнародний зв'язок або виставлення рахунків власникам безкоштовних міжміських номерів (Toll-free Numbers). Потім всі виклики концентруються на відповідних вузлах і передаються в корпоративні мережі. Однак через використання Інтернету в якості об'єднуючої магістралі, механізми захисту інформації стають життєво важливими елементами даної технології.

Як правило, віддалений користувач не має статичної адреси і підключається до захищається ресурсів не через виділений пристрій VPN, а за допомогою спеціального програмного забезпечення, що встановлюється на його комп'ютері.

Важливу роль при побудові VPN грають відносини підприємства з провайдером, зокрема, розподіл між ними функцій по конфігурації і експлуатації VPN-пристроїв.

При створенні захищених каналів VPN-засоби можуть розташовуватися як в середовищі обладнання провайдера, так і в обладнанні підприємства. Залежно від цього, виділяють два варіанти побудови VPN: призначена для користувача схема (Customer Provided VPN) і провайдерська схема (Provider Provisioned VPN).

Крім названої вище класифікації, всі варіанти створення VPN можна розділити на дві категорії: програмні і апаратні.

Програмні рішення являють собою готові програми, які встановлюються на час огляду мережі комп'ютера зі стандартним програмним забезпеченням.

Апаратні VPN-рішення включають в себе комп'ютер, операційну систему, спеціальне програмне забезпечення.

Віртуальні приватні мережі можна вважати повноцінним видом транспорту для передачі трафіку, тільки якщо є гарантії на пропускну здатність та інші параметри продуктивності, а також безпеку переданих даних.

1.2 Класифікація VPN

Існує декілька класифікацій VPN по різноманітним базовим параметрам.

За способом реалізації: Програмне рішення. Для функціонування VPN використовується ПК з спеціалізованим ПЗ.

Програмно-апаратне рішення. Для реалізації VPN використовується комплекс спеціальних програмно-апаратних засобів. За рахунок такого підходу забезпечується висока продуктивність та захищеність.

Інтегроване рішення. Реалізацію VPN забезпечує програмно-апаратний комплекс, який попутно вирішує задачі організації мережевого екрану, фільтрації трафіка і т.п.

За ступенем захищеності: Захищені. Це найпопулярніший вид VPN, за допомогою якого створюються захищені та надійні иережі на базі ненадійних мереж, наприклад, Інтернет.

За призначенням: Extranet VPN. Віртуальні мережі, в які можуть підключатися «зовнішні» користувачі — клієнти або замовники. Оскільки вони користуються меншою довірою, ніж співробітники компанії, існує необхідність створення певних правил, що обмежують доступ «зовнішних» користувачів до конфіденційної або комерційної інформації.

Remote Access VPN. Реалізується для забезпечення захищеного каналу між корпоративною мережею та користувачем, підключеним до захищеної мережі ззовні, наприклад, з домашнього ПК.

Internet VPN. Реалізується провайдерами для надання доступу клієнтам, що підключаються по одному фізичному каналу.

Intranet VPN. Об'єднує в захищену мережу ряд філій однієї компанії, розподілених географічно, для обміну інформацією по відкритим каналам.

Client / Server VPN. Захищає дані, що передаються між вузлами корпоративної мережі (але не мережами). Зазвичай реалізується для вузлів, що знаходяться в одному мережевому сегменті, наприклад, клієнтської машиною і сервером. Цей варіант застосовується для поділу однієї фізичної мережі на кілька логічних.

За типом протоколу: На ринку є реалізації VPN для мереж TCP/IP, AppleTalk та IPX. Проте найбільш актуальною вважається тенденція переходу на TCP/IP, тому більшість рішень підтримує тільки його.

Сьогодні існує декілька популярних реалізацій VPN, серед яких варто згадати PPTP, OpenVPN, L2TP, PPPoE, IPSec.

1.3 Функції VPN по захисту даних

Підключення будь-якої корпоративної мережі до публічної викликає два типи загроз:

- несанкціонований доступ до ресурсів локальної мережі, откриманий в результаті входу в цю мережу.
- несанкціонований доступ до даних при передачі трафіку по публічній мережі.

Віртуальні приватні мережі є комбінацією декількох самостійних сервісів (механізмів) безпеки:

- шифрування (з використання інфраструктури криптосистем) на виділених шлюзах (шлюз забезпечує обмін даними між обчислювальними мережами, що функціонують по різних протоколах);
- екранування (з використанням міжмережевих екранів);
- тунелювання.

При цьому узгоджуючим сторонам необхідна платформа підключення, яка не тільки швидко масштабується, а й (в першу чергу) забезпечує конфіденційність даних, цілісність даних і аутентифікацію.

Функції VPN по захисту даних полягають в наступному:

На всі комп'ютери, що мають вихід в Інтернет (замість Інтернет може бути і будь-яка інша мережа загального користування), встановлюється «VPN-агенти» - засіб, що реалізовує VPN, мережевий шлюз, які обробляють IP-пакети, що передаються по мережах.

Для корпоративного зв'язку в великих організаціях або об'єднання віддалених один від одного офісів для реалізації VPN-технологій в ролі шлюзу можуть виступати: сервера Unix, сервера Windows, мережевий маршрутизатор і мережевий шлюз на якому піднято VPN.

Перед відправкою IP-пакету «VPN-агент» виконує наступні операції:

- аналізується IP-адреса одержувача пакета, в залежності від цієї адреси вибирається алгоритм захисту даного пакету(VPN-агенти можуть, підтримувати одночасно кілька алгоритмів шифрування і контролю цілісності). Пакет може і зовсім бути відкинутий, якщо в настройках VPN-агента такий одержувач не значиться;
- обчислюється і додається в пакет його імітопріставка (криптографічний контрольна сума, розрахована з використанням ключа шифрування), що забезпечує контроль цілісності переданих даних;
- пакет шифрується (цілком, включаючи заголовок IP-пакета, що містить службову інформацію);
- формується новий заголовок пакета, де замість адреси одержувача вказується адреса його VPN-агента (ця процедура називається інкапсуляцією пакета).

В результаті цього, обмін даними між двома локальними мережами зовні представляється як обмін між двома комп'ютерами, на яких встановлені VPN-агенти. Будь-яка корисна для зовнішньої атаки інформація, наприклад, внутрішні IP-адреси мережі, в цьому випадку недоступна.

При отриманні IP-пакета виконуються зворотні дії:

- з заголовка пакета витягується інформація про VPN-агента відправника пакета, якщо такий відправник не входить в число дозволених, то пакет відкидається (те ж саме відбувається при прийомі пакету з навмисно або випадково пошкодженим заголовком);

- згідно з налаштуваннями вибираються криптографічні алгоритми і ключі, після чого пакет розшифровується і перевіряється його цілісність (пакети з порушеною цілісністю також відкидаються);
- після всіх зворотних перетворень пакет в його початковому вигляді відправляється справжньому адресату по локальній мережі.

Таким чином, інформаційний потік по громадській мережі передається по захищеному каналу. Для створення захищеного каналу кошти VPN використовують процедури шифрування, аутентифікації і авторизації.

Методів шифрування досить багато, тому важливо, щоб на кінцях тунелю використовувався один і той же алгоритм шифрування. Крім того, для успішного дешифрування даних джерела і одержувача даних необхідно обмінятися ключами шифрування. Слід зазначити, що шифрування повідомлень необхідно не завжди. Часто воно виявляється досить дорогою процедурою, що вимагає додаткових приставок для маршрутизаторів, без яких вони не можуть одночасно з шифруванням забезпечувати прийнятний рівень швидкодії.

Під аутентифікацією розуміється визначення користувача або кінцевого пристрою. Аутентифікація дозволяє встановлювати з'єднання лише між легальними користувачами і, відповідно, запобігає доступ до ресурсів мережі несанкціонованих користувачів.

У процедурі беруть участь дві сторони: одна доводить свою автентичність, а інша її перевіряє і приймає рішення.

Найчастіше для аутентифікації використовується пароль, але можуть застосовуватися і інші докази. Недоліками застосування паролів є їх розкриття, що частково компенсується їх простотою.

Аутентифікація даних свідчить про їх цілісності, а також про те, що вони надійшли від одного з учасників (при цьому використовується електронний підпис).

Авторизація передбачає надання абонентам різних видів послуг. Кожному користувачеві надаються певні адміністратором права доступу.

Ця процедура виконується після процедури аутентифікації і дозволяє контролювати доступ санкціонованих користувачів до ресурсів мережі.

Взагалі, процедури аутентифікації і авторизації виконують одну задачу і до них пред'являються однакові вимоги.

Цілісність переданих даних дозволяє забезпечити застосування електронного підпису.

1.4 Застосування тунелів для VPN

Для передачі даних VPN-агенти створюють віртуальні канали між захищеними локальними мережами або комп'ютерами (такий канал називається «тунелем», а технологія його створення називається «тунелювованням»).

На рис.1.2 представлений принцип роботи в режимі тунелю, в якому комп'ютери интрасетей можуть взаємодіяти з комп'ютерами інший интрасети шляхом маршрутизації пакетів через тунель IPsec між двома шлюзами.

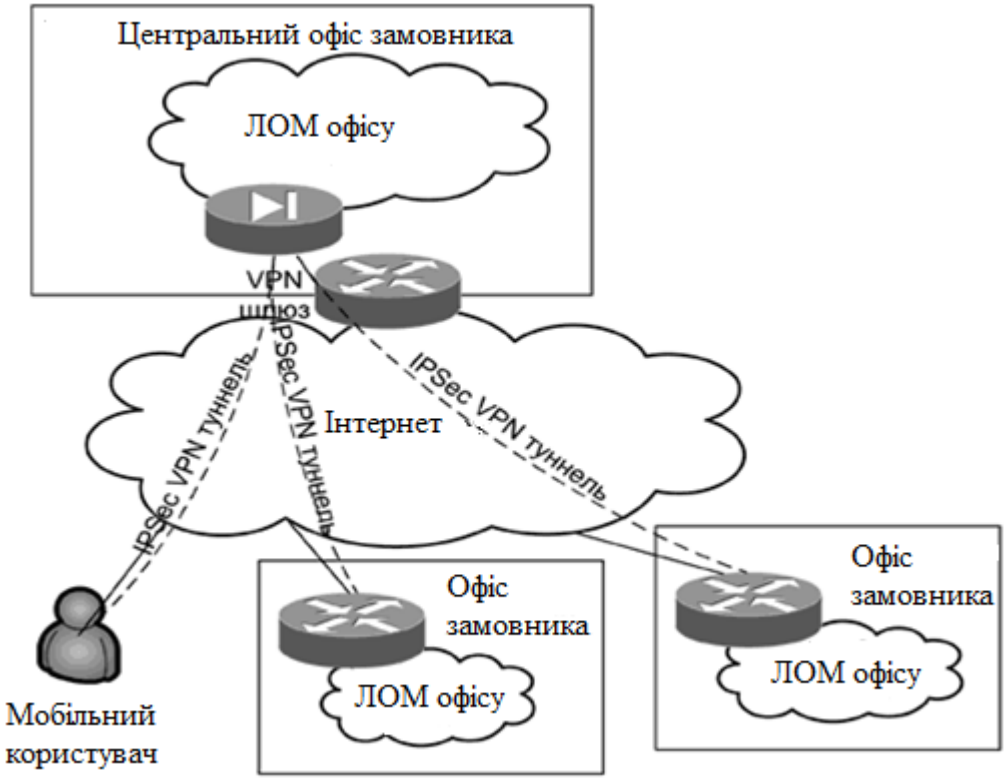


Рисунок 1.2 Принцип роботи в режимі тунелю

Протоколи захищеного каналу, як правило, використовують в своїй роботі механізм тунелювання. За допомогою даної методики пакети даних транслюються через загальнодоступну мережу як по звичайному двоточковому з'єднанню. Між кожною парою «відправник–отримувач даних» встановлюється своєрідний тунель – безпечне логічне з'єднання, яке дозволяє інкапсулювати дані одного протоколу в пакети іншого (рис.1.3).

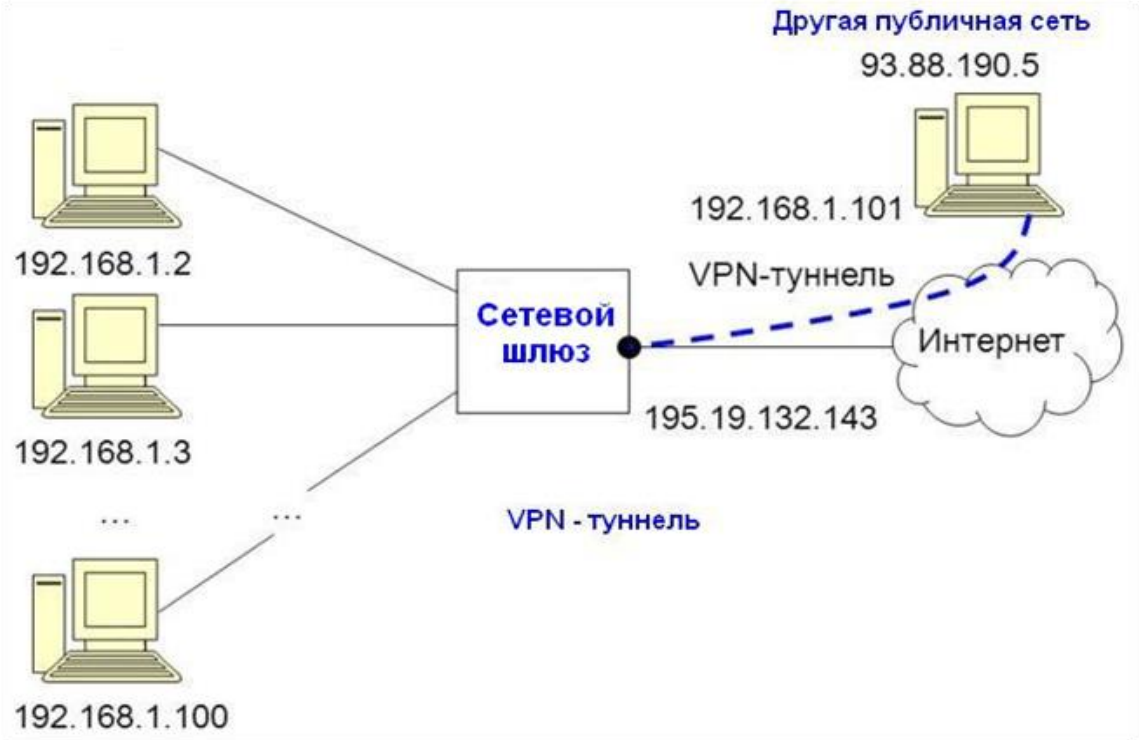


Рисунок 1.3 Приклад тунелювання

Сукупність правил створення тунелів, яка називається «політикою безпеки», записується в налаштуваннях VPN-агентів. IP-пакети направляються в той чи інший тунель або відкидаються після того, як будуть перевірені:

- IP-адреса джерела (для вихідного пакету - адреса конкретного комп'ютера мережі, що захищається);
- IP-адреса призначення;
- протокол більш високого рівня, якому належить даний пакет (наприклад, TCP або UDP);
- номер порту, з якого або на який відправлена інформація.

Процес тунелювання (або інкапсуляції) зводиться до того, що пакет протоколу нижчого рівня поміщається в поле даних пакета протоколу такого ж або більш високого рівня.

Цей механізм використовується для безпеки передачі даних через публічні мережі шляхом упаковки пакетів під зовнішню

оболонку. Тунель створюється між двома граничними пристроями, які розміщуються в точках входу в мережу.

Рисунок 1.4 Приклад тунелю

Технологія тунелювання дозволяє зашифрувати вихідний пакет повністю, разом із заголовком, а не тільки його поле даних. Такий зашифрований пакет поміщається в інший пакет з відкритим заголовком. Цей заголовок використовують для транспортування даних на ділянці загальної мережі. У граничнійі точці захищеного каналу витягується зашифрований заголовок, який буде використовуватися для подальшої передачі пакета.

Як правило, тунель створюється тільки на ділянці мережі загального користування, де існує загроза порушення конфіденційності і цілісності даних.

Крім захисту переданої інформації механізм тунелювання використовують для забезпечення цілісності та автентичності. При цьому, захист потоку реалізується більш повно. Тунелювання застосовується також і для узгодження різних транспортних технологій, якщо дані одного протоколу транспортного рівня необхідно передати через транзитну мережу з іншим транспортним протоколом.

Для формування тунелів VPN використовують протоколи PPTP, L2TP, IPsec, IP-IP. Протокол PPTP дозволяє інкапсулювати IP-, IPX-і NetBEUI-трафік в заголовки IP для передачі по IP-мережі, наприклад, Internet.

Протокол L2TP дозволяє шифрувати и передавати IP-трафік з використанняи будь-якіх протоколів, що підтрімують режим "точка-точка" доставки дейтаграм. Наприклад, до них відносяться протокол IP, ретрансляція кадрів и асинхронний режим передачі (ATM). Протокол IPsec - дозволяє шифрувати та інкапсулювати корисну інформацію протоколу IP в заголовки IP для передачі по IP-мережі.

Модель OSI	Протоколи захищеного каналу
Прикладний	MIME
Представлення	SSL, TLS
Сеансовий	
Транспортний	
Мережевий	IPSec
Канальний	PPTP
Фізичний	

Рисунок 1.5 Протоколи захищеного каналу в моделі OSI

1.5 Технології створення віртуальних приватних мереж

На організацію віртуальних мереж впливають різні чинники, одним з них є вибір технології побудови VPN.

Серед технологій побудови VPN можна назвати такі технології як: IPSec VPN, MPLS VPN, VPN на основі технологій тунелювання PPTP, L2TP. У всіх перерахованих випадках трафік надсилається в мережу провайдера за протоколом IP, що дозволяє провайдеру надавати не тільки послуги VPN, але і різні додаткові сервіси (контроль за роботою

клієнтської мережі, хостинг Web і поштових служб, хостинг спеціалізованих додатків клієнтів).

На рисунку 1.6 представлений загальний варіант побудови віртуальної приватної мережі на базі загальнодоступної мережі провайдера. Мережа кожного клієнта складається з територіально розподілених офісів, які пов'язані між тунелями, прокладеними через мережу провайдера.

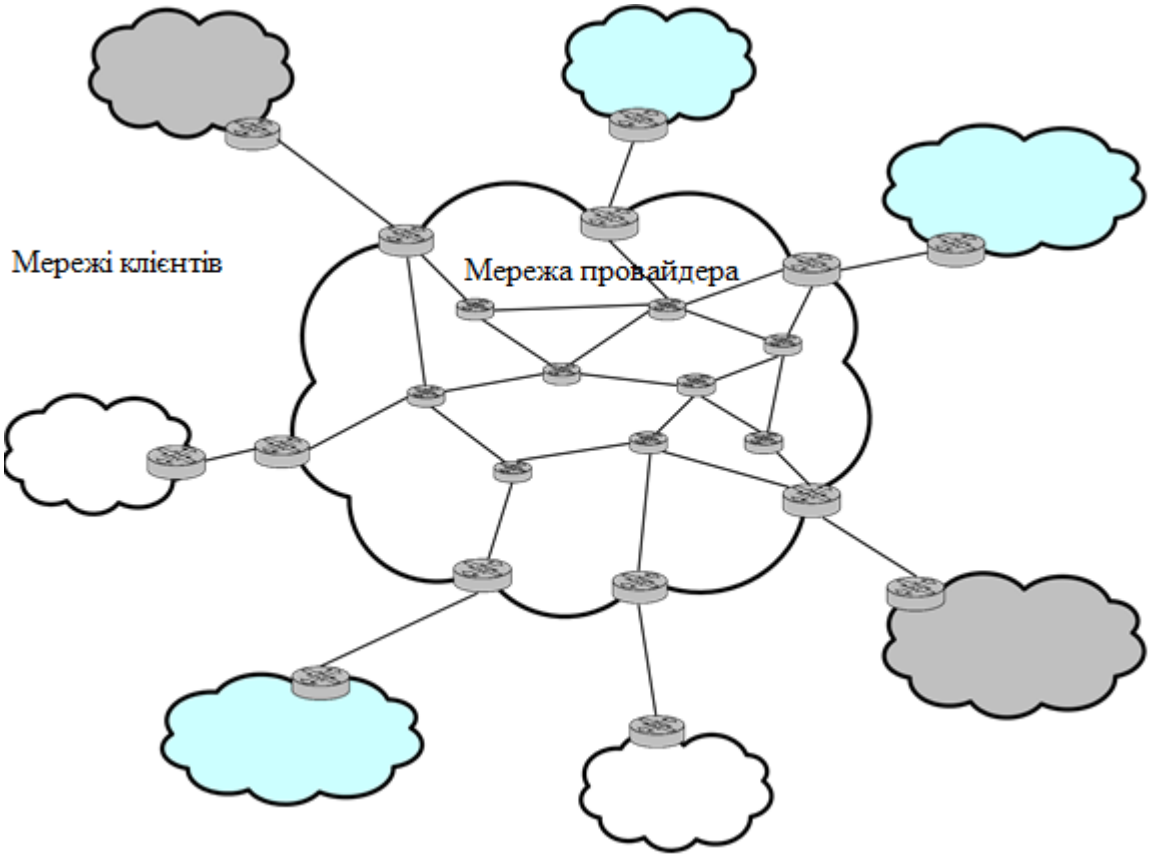


Рисунок 1.6 Віртуальна приватна мережа

Internet Protocol Security відноситься до найбільш поширених і популярних технологій VPN. Стандарт IPSec забезпечує високий ступінь гнучкості, дозволяючи вибирати потрібний режим захисту, а також дозволяє використовувати різні алгоритми аутентифікації і шифрування даних. Режим інкапсуляції пакетів дозволяє ізолювати адресні простори

клієнта і провайдера за рахунок застосування двох IP адрес: зовнішнього і внутрішнього.

IPSec, як правило, застосовується для створення VPN, підтримуваних провайдером, - тунелі в них будуються на базі пристроїв клієнта, але конфігуруються вони віддалено і управляються провайдером.

Технологія IPSec дозволяє вирішувати такі завдання щодо встановлення і підтримання захищеного каналу:

- аутентифікацію користувачів або комп'ютерів при ініціалізації каналу.
- шифрування і аутентифікацію переданих даних між кінцевими точками каналу.
- автоматичне постачання точок секретними ключами, необхідними для роботи протоколів аутентифікації і шифрування даних.

Недоліком даної технології є той факт, що з усіх властивостей віртуальної мережі технологія IPSec реалізує тільки захищеність та ізольованість адресного простору. Пропускну здатність і інші параметри QoS вона не підтримує. Крім того, мінусом IPSec є і його орієнтованість виключно на IP-протокол.

VPN на основі тунелювання через IP: сюди входять всі технології, для створення VPN, які використовують тунелі через IP-мережі. Застосування тунелю дозволяє ізолювати адресний простір клієнта, що в свою чергу дає клієнтові можливість переносити незашифрований трафік (L2TP) або шифрувати його (PPTP).

Протокол PPTP підтримує управління потоками даних і багато протокольне тунелювання на базі протоколу IP. Віддаленим користувачам протокол дозволяє отримувати доступ до корпоративної мережі, підключаючись по телефонній лінії до місцевого постачальника послуг

Інтернет замість прямого підключення до мережі компанії. PPTP забезпечує з'єднання з потрібним сервером, створюючи для кожного віддаленого клієнта віртуальну мережу. Протокол вирішує багато проблем мережевих адміністраторів, змушених забезпечувати підтримку безлічі віддалених користувачів, але бажаючих уникнути створення і обслуговування відносно дорогих мереж на виділених каналах.

Специфікації L2TP розробляє IETF. Він орієнтований на підтримку багато протокольного тунелювання, але крім цього, забезпечує сумісність всіх L2TP продуктів.

До недоліків протоколів PPTP і L2TP можна віднести відсутність вбудованих алгоритмів шифрування.

Технологія MPLS VPN в даний час, є однією з найбільш перспективних технологій створення VPN.

Мережа MPLS VPN ділиться на дві області: IP-мережі клієнтів і внутрішня (магістральна) мережа провайдера, яка служить для об'єднання клієнтських мереж.

У загальному випадку, у кожного клієнта може бути кілька територіально відокремлених мереж IP, кожна з яких в свою чергу може включати декілька підмереж, пов'язаних маршрутизаторами. Такі територіально ізольовані мережеві елементи корпоративної мережі прийнято називати сайтами. Належать одному клієнту сайти обмінюються IP пакетами через мережу провайдера MPLS і утворюють віртуальну приватну мережу цього клієнта. Обмін маршрутної інформацією в межах сайту здійснюється по одному з внутрішніх протоколів маршрутизації IGP.

Структура MPLS VPN передбачає наявність трьох основних компонентів мережі:

- Customer Enge Router, CE - граничний маршрутизатор клієнта.

- Provider Router, P - внутрішній маршрутизатор магістральної мережі провайдера.
- Provider Enge Router, PE – граничний маршрутизатор мережі провайдера.

Граничні маршрутизатори клієнта служать для підключення сайту клієнта до магістральної мережі провайдера. Ці маршрутизатори належать мережі клієнта і нічого не знають про існування VPN. До граничних маршрутизаторів мережі провайдера через маршрутизатори CE сайти клієнтів і внутрішні маршрутизатори мережі провайдера. Взаємодія маршрутизаторів CE і PE реалізується на основі стандартних протоколів стека TCP / IP.

CE-маршрутизатори різних сайтів не обмінюються маршрутною інформацією безпосередньо і навіть можуть не знати один про одного. Адресні простори підмереж, що входять до складу VPN можуть перекриватися, тобто унікальність адрес повинна дотримуватися тільки в межах конкретної підмережі. Це вдалося домогтися перетворенням IP-адреси в VPN-IP-адреса і використанням протоколу MP-BGP для роботи з цими адресами. Вважається, що CE-маршрутизатор відноситься до одного сайту, але сайт може належати до кількох VPN. До PE-маршрутизатора може бути підключено кілька CE-маршрутизаторів, що знаходяться в різних сайтах і навіть відносяться до різних VPN.

Маршрутизатори CE не зобов'язані підтримувати технологію багатопротокольної комутації, підтримка MPLS потрібна тільки для внутрішніх інтерфейсів PE маршрутизаторів і, звичайно, для всіх інтерфейсів маршрутизаторів P.По функціональній побудові більш складними являються граничні маршрутизатори мережі провайдера. На них покладається функція підтримки VPN, а саме: розмежування маршрутів і даних, що надходять від різних клієнтів. Крім того, ці

маршрутизатори служать кінцевими точками шляхів LSP між сайтами замовника.

Кожен PE-маршрутизатор повинен підтримувати стільки таблиць маршрутизації, скільки сайтів користувачів до нього приєднано, тобто на одному фізичному маршрутизаторі організується кілька віртуальних. Причому маршрутна інформація, що стосується конкретної VPN, міститься тільки в PE маршрутизаторах, до яких під'єднані сайти даної VPN. Таким чином вирішується проблема масштабування, яка неминуче виникає в разі наявності цієї інформації в усіх маршрутизаторах мережі оператора.

Під кожен новий сайт клієнта PE створює окрему асоційовану таблицю маршрутизації.

Кожній асоційованій таблиці маршрутизації в маршрутизаторі PE присвоюється один або кілька атрибутів RT, які визначають набір сайтів, що входять в конкретну VPN. Крім цього, маршрут може бути асоційований з атрибутом VPN of Origin, однозначно ідентифікує групу сайтів і відповідний маршрут, оголошений одним з маршрутизаторів, що знаходяться в цих сайтах; і з атрибутом Site of Origin, що ідентифікує сайт, від якого маршрутизатор PE отримав інформацію про даному маршруті.

Через маршрутизатори PE проходить невидима межа між зоною клієнтських сайтів і зоною ядра провайдера. По один бік розташовуються інтерфейси, через які PE взаємодіє з маршрутизаторами P, а по іншу - інтерфейси, до яких підключаються сайти клієнтів. З одного боку на PE надходять оголошення про маршрутах магістральної мережі, з іншого боку - оголошення про маршрутах в мережах клієнтів.

Обмеження області поширення маршрутної інформації межами окремих VPN ізолює адресні простори кожної VPN, дозволяючи застосовувати в її межах як публічні адреси Інтернет, так і приватні (private) адреси. Всім адресам адресного простору однієї VPN додається

префікс, званий розрізнювачем маршрутів (Route Distinguisher, RD), який унікально ідентифікує цю VPN. В результаті, на маршрутизаторі PE все адреси, що відносяться до різних VPN, обов'язково будуть відрізнятися один від одного, навіть якщо вони мають частину, що збігається – IP-адреса.

Обмін маршрутної інформації між сайтами кожної окремої VPN виконується під управлінням протоколу MP-BGP (Multiprotocol BGP).

MPLS не забезпечує безпеку за рахунок шифрування і аутентифікації, як це робить IPSec, але допускає застосування даних технологій як додаткових заходів захисту. Провайдер MPLS може пропонувати клієнтам послуги гарантованої якості обслуговування при використанні методів Traffic Engineering або DiffServ.

Віртуальні мережі VPN MPLS орієнтовані на побудову захищеної корпоративної мережі клієнта на базі приватної мережевої інфраструктури однієї компанії. Даний варіант організації поєднує в собі переваги застосування протоколу IP з безпекою приватних мереж і наданих якістю обслуговування, які дає технологія MPLS.

Мережі MPLS VPN найбільше підходять для створення корпоративного простору для електронної комерції, що забезпечує єдине мережеве середовище для підрозділів корпорації і організацію екстрамережі. Вони також можуть стати основою для електронної комерційної діяльності підприємства.

1.6 Висновки з розділу 1

VPN (Virtual Private Network) — це віртуальна приватна мережа або логічна мережа, яка створюється поверх незахищених мереж. VPN класифікують за: способом реалізації, ступенем захищеності, призначенням, типом протоколу. Віртуальні приватні мережі виконують

функції шифрування, екранування, тунелювання. Для формування тунелів VPN використовують протоколи PPTP, L2TP, IPsec, IP-IP. Технологія MPLS VPN в даний час, є однією з найбільш перспективних технологій створення VPN.

2 АНАЛІЗ ОСНОВНИХ ТЕХНІЧНИХ РІШЕНЬ ТЕХНОЛОГІЙ VPN

2.1 Огляд принципів роботи MPLS VPN

MPLS стала основною магістральної технологією нового століття. Вона дозволяє ефективніше передавати великі об'єми трафіку в магістральних мережах і розглядається як основа для конвергенції послуг і фундамент для побудови мультисервісних мереж наступного покоління, в яких стане можлива передача різнорідного трафіку через інтегровану телекомунікаційну інфраструктуру замість декількох раздічних мереж. У сфері майбутніх телекомунікацій MPLS приготована роль провідної технології. Вона розглядається в якості фундаменту для інфраструктури мереж наступного покоління і надання нових послуг. Володіючи цілим рядом переваг, вона була покликана доповнити «світ IP» перевагами успадкованих інфраструктур frame relay, ATM і TDM, а також сприяти впровадженню протоколу IP як універсального транспорту для всіх видів додатків. У разі застосування MPLS в якості базового механізму комутації можна спростити розвиток операторських мереж IP, об'єднати різні технології доступу, підвищити масштабованість маршрутизації IP і зробити мережі IP настільки ж придатними для передачі голосу і відео, як мережі ATM, де забезпечення якості та резервування ресурсів для передачі різнорідного трафіку закладені на протокольному рівні. При тому, що оператори досить виважено підходять до технології MPLS, популярність її зростає. Багатопротокольна комутація інформаційних потоків відповідно до мітками (Multiprotocol Label Switching, MPLS) розглядається як перспективна, хоча і не єдина основа для конвергенції послуг і побудови мультисервісних мереж наступного покоління (NGN), в яких стане можлива передача різнорідного трафіку через інтегровану телекомунікаційну інфраструктуру замість декількох різних мереж. Прийняття MPLS в якості уніфікованої, замісної технології повинно

привести до значного спрощення мережевих інфраструктур і управління ними. Впровадження MPLS дозволяє підвищити рівень сервісу, надавати послуги, якы мають високий попит, на базі IP (з гарантованим рівнем якості) і послуги конвергентних мереж для корпоративних клієнтів, включаючи створення віртуальних приватних мереж (VPN) і передачу голосу поверх IP (VoIP). Інфраструктура MPLS VPN дає можливість з'єднувати вузли за схемою «будь-який з будь-яким» незалежно від технології доступу (frame relay, виділена лінія, DSL або Ethernet), підвищує продуктивність, масштабованість IP і надійність маршрутизації в додатках Triple Play (голос, дані, відео). З MPLS добре поєднується Ethernet - завдяки такій комбінації відкривається можливість економічного надання цілого комплексу послуг і впровадження широкосмугових додатків в міських мережах і мережах доступу.

Кожен пакет при використанні на мережевому рівні протоколу, який не передбачає створення віртуальних з'єднань, на своєму шляху проходження передається незалежно від одного маршрутизатора до іншого. Відповідно, при визначенні маршруту прямування пакету кожен маршрутизатор витрачає свої ресурси на аналіз IP-заголовку. Можливість уникнути цих витрат дозволяє реалізувати передачу пакетів по мережі значно швидше.

Як технології, що забезпечує прискорену передачу пакетів по мережі, застосовується технологія MPLS. MPLS (Multiprotocol Label Switching) - це технологія багатопротокольної комутації на основі міток.

Основною цінністю технології MPLS є можливість організації в IP мережі «віртуальних каналів», а також можливість перенесення трафіку однієї сесії по декільком «віртуальним каналам».

«Multiprotocol» в назві технології означає мультипротокольний. Це говорить про те, що технологія MPLS може бути застосована до будь-якого протоколу мережевого рівня, тобто MPLS - це свого роду

інкапсулюючий протокол, здатний транслювати інформацію безлічі інших протоколів вищих рівнів моделі OSI. Технологія MPLS залишається незалежною від протоколів рівнів 2 і 3 в мережах IP, ATM і Frame Relay, а також, взаємодіє з існуючими протоколами маршрутизації, такими як протокол резервування ресурсів RSVP або мережевий протокол переважного вибору найкоротших маршрутів OSPF.

Комітет IETF визначив три основні елемента технології MPLS:

- Мітка
- FEC - клас еквівалентної пересилання
- LSP - комутований по мітках тракт.

Мітка - це ідентифікатор фіксованої довжини, що визначає клас еквівалентного пересилання FEC. Мітки мають локальне значення, тобто прив'язка мітки до FEC використовується тільки для пари маршрутизаторів. Мітка використовується для пересилки пакетів від верхнього маршрутизатора до нижнього, де, будучи вхідною, замінюється на вихідну мітку, що має також локальне значення на наступній ділянці шляху.

Протокол MPLS підтримує різні типи міток: це може бути 4-байтовая мітка MPLS, яка вставляється між заголовками канального і мережевого рівня. Це може бути мітка ідентифікаторів віртуального каналу і віртуального шляху (VCI / VPI) або мітка ідентифікатора з'єднання канального рівня (DLCI).

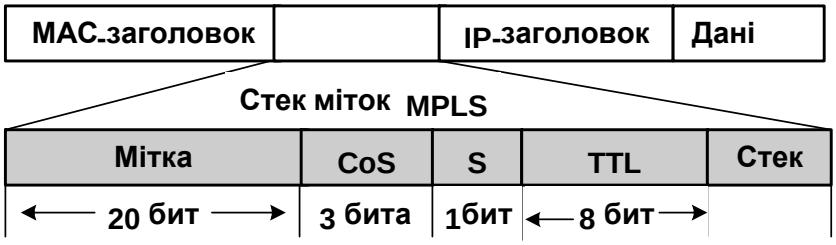


Рисунок 2.1 Стек міток

Розмір мітки становить 4 байта. Ідентифікатор самої мітки займає перші 20 біт.

Інформація про рівень якості обслуговування в мережі MPLS може передаватися в поле CoS, що займає наступні три біта в поле мітки.

Останній біт (S) третього байта використовується для вказівки закінчення стека міток.

Четвертий байт в форматі поля мітки займає параметр TTL (Time to Live), який обмежує граничний час, існування пакету в мережі, для захисту від утворення петель і обмеження області розповсюдження пакета.

Стек міток

Пакет, який передається по мережі MPLS, як правило, містить не одну, а кілька міток. Такий набір міток утворює стек. Основне призначення стека міток - підтримка деревоподібності безлічі трактів LSP, що закінчуються в одному вхідному LSR, а, крім того, в тому, щоб використовувати мітки при створенні так званих LSP-тунелів.

Властивість деревоподібності зводиться до наступного: якщо в одному LSR зливається кілька потоків пакетів, то цей LSR не замінює мітки, пов'язані з цими потоками, а залишає їх, поміщуючи зверху мітку нового FEC, який відповідає об'єднаному потоку пакетів, що утворюється в результаті злиття.

Мітки в стеці розташовуються за принципом «останній прийшов - перший вийшов». Кожен маршрутизатор працює тільки з верхньої міткою.

Решта мітки стека передаються прозоро до видалення вищестоящої.

Для переадресації пакета, що надходить на один з інтерфейсів маршрутизатора, необхідно проведення двох процедур:

- По-перше, необхідно визначити наступний крок маршрутизації.

• По-друге, потрібно знати, яка операція потрібна для стека міток. Це може бути операція вилучення мітки з стека, заміни мітки в стек.

Після того, як з стека міток буде видалена остання мітка, подальша обробка пакетів повинна здійснюватися на основі заголовка мережевого рівня.

Для створення таблиць комутації по мітках використовуються різні методи:

• метод на основі топології. Для створення таблиць в цьому випадку використовуються стандартні протоколи маршрутизації. До таких протоколів відносяться OSPF, IS-IS, BGP.

• метод на основі запитів. Даний метод заснований на роботі керуючого протоколу, на основі запитів (наприклад, протокол RSVP).

• метод на основі трафіку. В даному варіанті створення міток процедура призначення і розподілу міток запускається тільки після надходження пакету.

Клас еквівалентного пересилання FEC

FEC - це форма подання групи пакетів з однаковими вимогами до передачі по мережі.

Як говорилося раніше, в заголовку IP-пакета міститься набагато більше інформації, ніж потрібно для вибору наступного маршрутизатора. Цей вибір можна організувати шляхом виконання наступних двох груп функцій в маршрутизаторі:

- маршрутизатор відносить пакет до певного класу FEC.
- ставить у відповідність кожному FEC наступний крок маршрутизації.

У MPLS пакет ставиться у відповідність певного класу FEC тільки один раз на вході в мережу MPLS. Цьому FEC присвоюється мітка,

передана потім разом з пакетом при його пересиланні до наступного маршрутизатора.

Клас FEC являє собою набір FEC-елементів, кожен з яких ідентифікується певною міткою. При співвіднесенні пакетів з різних FEC велику роль відіграють IP-адреси, пріоритети обслуговування та інші параметри трафіку. Кожен FEC обробляється окремо, що дозволяє підтримувати необхідну якість обслуговування в мережі MPLS.

Комутований по мітках тракт LSP

Комутований по мітках тракт - це послідовність MPLS маршрутізаторов і послідовність міток в них. По суті, LSP представляє собою віртуальний канал в мережі передачі даних.

Набір пакетів, що передається по LSP, відноситься до одного FEC, і кожен маршрутизатор LSR в LSP призначає для нього свою мітку. Іноді потік даних може бути настільки великий, що для нього створюється кілька LSP між відправником і отримувачем.

Можливі два варіанти створення LSP: за принципом hop-by-hop, який передбачає, що кожен маршрутизатор самостійно вибирає подальший шлях прямування пакета, або за принципом явної маршрутизації, в якому маршрутизатори передають пакет відповідно до вказівок, отриманими від верхнього, в даному тракті , LSR. Таким чином, в першому випадку маршрут проходження пакетів визначається випадковим чином, а в разі явної маршрутизації він відомий заздалегідь.

В мережі MPLS може існувати набір маршрутизаторів, які є вхідними для конкретного FEC, тоді, вважається, що для цього FEC існує LSP з різними точками входу і виходу. Якщо для деяких з цих LSP вихідним є один і той же LER, то можна говорити про дерево LSP, коренем якого є даний вихідний маршрутизатор.

LSP можна розглядати як тракт, створюваний шляхом зчеплення одного і більше ділянок маршруту, який дозволяє пересилати пакет,

замінюючи на кожному вузлі мережі MPLS вхідну мітку вихідною міткою (так званий алгоритм перестановки міток). Таким чином, тракт мережі MPLS можна розглядати як тунель, для створення якого в IP-пакет вставляється заголовок - мітка, про який йшлося раніше.

LSP встановлюються або перед передачею даних (з управлінням від програми), або при виявленні певного потоку даних (керовані даними LSP).

На сьогоднішній день застосування тунелювання реалізовано в багатьох технологіях. Утворення в віртуальному тракті тунелів, по яких проходять інші віртуальні тракти, ґрунтується на інкапсуляції переданих пакетів в пакети, що слідують по цьому тракту до даної адреси призначення. LSP-тунелі, що широко використовуються в технологіях підтримки широкосмугових послуг в MPLS будуть докладніше розглянуті після опису принципів функціонування мережі MPLS.

Будь-який IP-пакет на вході в мережу MPLS, незалежно від того надходить цей пакет від відправника або ж він прийшов з суміжної мережі, яка може бути MPLS-мережею більш високого рівня, відноситься до певного класу еквівалентного пересилання FEC (Forwarding Equivalence Class). Аналіз заголовка IP-пакета і призначення FEC проводиться тільки один раз на вході в мережу.

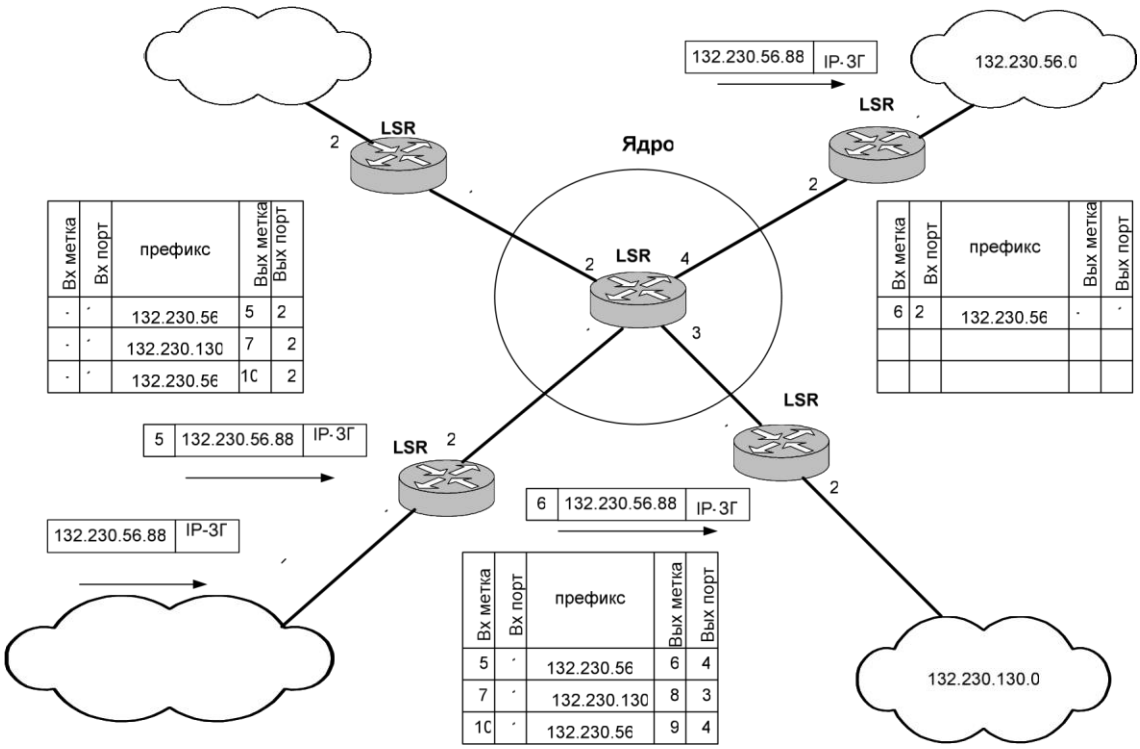


Рисунок 2.2 Мережа MPLS

FEC ідентифікується певною міткою, що представляє собою поле фіксованої довжини і має локальне значення на ділянці між двома сусідніми маршрутизаторами. При переадресації пакета на наступному кроці, мітка надсилається разом з ним, таким чином, пакети виявляються поміченими ще до того, як будуть переадресовані. Прийнята з пакетом мітка використовується маршрутизатором як покажчик входу таблиці, яка визначає черговий маршрутизатор для пересилання до нього пакету, а також нову мітку для FEC, до якого відноситься цей пакет. Модуль комутації по мітках, як правило, замінює в пакеті мітку,що міститься в ньому деякою нової міткою перед її пересиланням на наступну ділянку маршруту (label swapping). Для прийняття рішення про те, куди пересилати пакети, використовується алгоритм точного збігу міток.

Використання мітки для переадресації пакетів в MPLS дозволяє значно знизити час обробки пакетів в маршрутизаторі.

Маршрутизатор, що підтримує MPLS і здатний, крім того, аналізувати заголовки і виробляти пересилання пакетів, що не містять міток, називається маршрутизатором комутації по мітках. Технологія MPLS передбачає наявність маршрутизаторів двох типів:

- LER (Label Enge Routers) – граничні маршрутизатори MPLS.
- LSR (Label Switching Routers) – транзитні маршрутизатори MPLS.

У точці входу в мережу MPLS стоять граничні маршрутизатори, на які покладаються функції класифікації пакетів за різними класами FEC і реалізація різноманітних додаткових послуг. Вхідний LER додає мітку всіх пакетів, що надходять в мережу MPLS, а вихідний LER видаляє мітку і, або здійснює маршрутизацію на основі IP-адреси, або сам є адресатом. Таким чином, щоб переадресовувати пакети, LSR повинен вміти працювати з IP-заголовком.

Завдання транзитних маршрутизаторів MPLS полягає в просуванні пакетів на основі міток, тобто, маршрутизатор повинен прийняти пакет із вставленою міткою, у відповідності зі своєю таблицею маршрутизації замінити її новою і відправити пакет до наступного LSR.

Будь-який маршрутизатор MPLS містить базу міток LIB, завдяки якій пакети і маршрути зв'язуються між собою. Для отриманої мітки в базі LIB міститься точни й запис про відповідну вихідну мітку, інтерфейс і інформації про інкапсуляцію канального рівня, що необхідна для просування пакета. Грунтуючись на інформації, отриманої з бази LIB, LSR замінює отриману ним вхідну мітку на вихідну і передає пакет на вихідний інтерфейс. Ця операція повторюється при проходженні кожного LSR маршрутизатора.

Коли в LIB декількох LSR накопичується інформація, що відноситься до одного і того ж пункту призначення, створюється так званий «комутований по мітках тракт», що представляє собою

послідовність вузлів міток в вузлах на шляху проходження потоку від відправника до одержувача. Тракт LSP між двома маршрутизаторами є односпрямованим.

Для реалізації маршрутизації в мережі MPLS необхідно заповнити таблиці маршрутизації. Алгоритм маршрутизації працює по протоколу OSPF, IS-IS або BGP, або за допомогою явної маршрутизації. Після вибору оптимального маршруту маршрутизатори розподіляють по ньому мітки. Мітки в LSP роздаються за допомогою протоколу розподілу міток LDP.

Високошвидкісна передача даних в MPLS забезпечується за рахунок того, що мітки фіксованої довжини вставляються на початку пакета і можуть використовуватися апаратними засобами для швидкої комутації пакетів між каналами зв'язку.

При комутації пакетів можливий випадок, коли маршрутизатор отримує пакет з вхідною міткою, якої немає в його базі LIB. У таких ситуаціях пакет відкидається. Також можливі випадки, коли пакет надходить на маршрутизатор, в якому з якоїсь причини не може бути встановлений зв'язок між вхідною та вихідною мітками. У цій ситуації можливі два виходи. По-перше, можна продовжити маршрутизацію пакетів традиційним способом. Але цей варіант рішення підходить не завжди, так як може привести до утворення петель, та й змісту IP-заголовка мало для переадресації пакета. В силу цих обставин пріоритетним є другий варіант - відкидання пакету.

Заміна міток

Для переадресації пакетів, що містять мітки, LSR аналізує верхню мітку стека і на основі FEC цього пакета, а також LIB, приймає рішення про подальший шлях прямування пакета. Якщо пакет є непоміченим, тобто не містить в собі стека міток, то маршрутизація пакету проводиться

на основі IP-заголовку, визначаючи, таким чином, клас еквівалентності пакета. Потім, маршрутизатор визначає маршрут пакета.

Від маршрутизатора MPLS потрібно, щоб він міг зв'язати набір вхідних міток з однією вихідною. Дана процедура називається об'єднанням міток. LSR здатний об'єднувати мітки, якщо він при отриманні пакетів з різними вхідними мітками пересилає їх з однієї і тієї ж вихідною міткою. При цьому, інформація про те, що вони прийшли від різних інтерфейсів втрачається.

В архітектурі MPLS допускається наявність як об'єднуючих і не об'єднуючих маршрутизаторів, так і маршрутизаторів, що не підтримують комутацію на основі міток.

Тунелі в MPLS

LSP-тунель являє собою послідовність <LSR1, LSR2, ..., LSRn>, в якому LSR1 є передавальним кінцевим пунктом тунелю, а LSRn - прийомним кінцевим пунктом тунелю. Пакети, що підлягають транспортуванню через LSP-тунель, відносяться до одного FEC, і кожен LSR тунелю призначає мітку для цього FEC, тобто мітку для тунелю. Щоб направити пакет в LSP-тунель, маршрутизатор передавального кінцевого пункту тунелю поміщає позначку, призначену для цього тунелю, на існуючому в пакеті стека міток (зауважимо, що і в даному випадку передостанній маршрутизатор LSP-тунелю може знищити верхню мітку в стеці до передачі пакета до приймального пункту призначення).

LSP-тунель створюється всередині LSP. Істотно, що початок і / або кінець тунелю, як правило, не збігаються з початком і / або кінцем цього LSP, тунель зазвичай буває коротше LSP, в якому він створений. В одному LSP може бути створено кілька LSP-тунелів одного рівня з незбіжними передавальними і / або прийомними кінцевими пунктами. Більш того, всередині кожного з цих тунелів можна створювати LSP-тунелі наступного рівня. Кількість таких рівнів, з тих чи інших причин, не

може бути скільки завгодно великим, проте ієрархічність архітектури MPLS в даному випадку цілком очевидна. Здійснюється вона за допомогою стека міток. Механізм стека міток дозволяє здійснювати ієрархічне функціонування в мережі MPLS. Він, зокрема, дозволяє використовувати MPLS для здійснення одночасно маршрутизації як між окремими маршрутизаторами всередині мережі даного Інтернет-провайдера, так і високорівневою міждоменною маршрутизацією. Кожен рівень в стеці міток відноситься до деякого ієрархічному рівню, що полегшує підтримку тунелювання в MPLS.

Під LSP рівня m розуміється LSP, що утворюється послідовністю маршрутизаторів <LSRвх, LSR2, ..., LSRn-1, LSRвих> з наступними властивостями:

- вхідний маршрутизатор $LSR_{вх}$ поміщає в стек міток оброблюваного пакета таку по рахунку мітку, що стек набуває глибини m;
- при всіх i ($1<i<n$) пакет, що надходить до LSR_i, має стек міток глибини m;
- в процесі транспортування пакета від $LSR_{вх}$ до LSR_{n-1} глибина його стека міток ніколи не буває менше m;
- при всіх i ($1<i<n$) LSR_i передає пакет LSR_{i+1} засобами MPLS.

Іншими словами, LSP рівня m являє собою послідовність маршрутизаторів, яка починається з вхідного LSR, вставляє в пакет мітку рівня m, містить проміжні LSR, кожен з яких приймає рішення про пересилку пакету на основі мітки рівня m, і закінчується вихідним LSR, де рішення про пересилання приймається на основі мітки рівня m - k, де $k> 0$, або на основі звичайних (НЕ MPLS) процедур пересилання. Відзначимо, що від LSRn-1 до LSRn можна передавати пакети зі стеком міток глибини (m-1), оскільки мітка рівня m вихідного LSR не потрібна. Це дозволяє

позбавити вихідний LSR від операцій аналізу непотрібної йому мітки і не вимагає ніяких додаткових операцій, крім простого знищення в передостанньому LSR верхньої мітки в стеці. Тобто, в мережі MPLS можуть утворюватися LSP-тунелі довільного ступеня складності. Якщо оператор повинен вкласти один LSP-тунель в інший LSP-тунель, то потоку призначається розглянутий вище стек міток, як це показано на рисунку 2.3. У таких випадках MPLS-мітки поміщаються в стек міток на вході в кожен тунель і витягуються з стека міток на виході з тунелю. Остання мітка з стека буде залучена тоді, коли потік прийде на граничний маршрутизатор на шляху до адресата.

Таким чином, шляхом створення тунелів через кілька мережевих сегментів досягається унікальна можливість MPLS управляти всім трактом передачі пакета без специфікацій в явному вигляді проміжних маршрутизаторів. У зв'язку з цим розглянемо кілька більш загальну схему, представлену на рисунку 2.4.

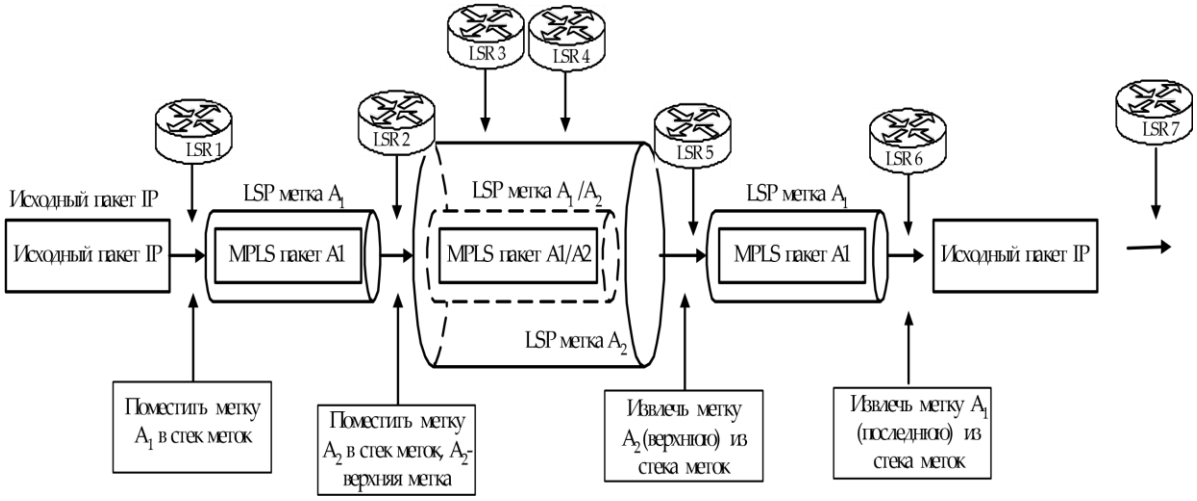


Рисунок 2.3 Тунелювання через LSP

Нехай тут всі граничні маршрутизатори MPLS (LSR1, LSR2, LSR3 і LSR4) використовують протокол BGP і створюють комутований по мітках тракт LSP між ними (LSP1). LSR1 знає про те, що його наступний пункт призначення - LSR2, оскільки він передає дані від відправника, які повинні

пройти через два сегмента мережі. У свою чергу, LSR2 знає про те, що його наступний пункт призначення - LSR3, і т.д. Ці граничні LSR використовуватимуть протокол LDP для отримання і зберігання міток від вихідного LSR4 аж до вхідного LSR1.

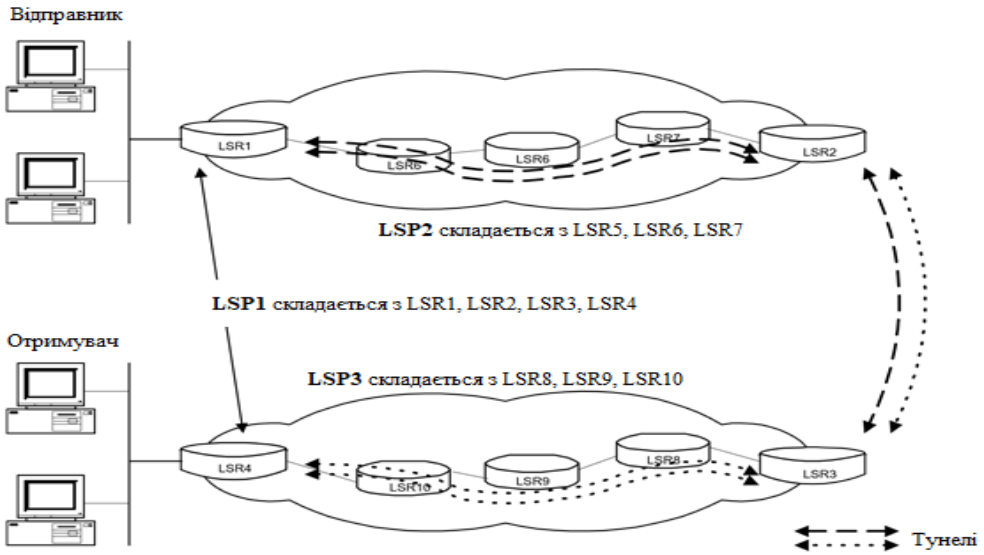


Рисунок 2.4 Тунелі в мережі MPLS

Однак, щоб дані були передані від LSR1 до LSR2, вони повинні пройти через кілька (в даному випадку три) транзитних маршрутизаторів LSR. Таким чином, між двома LSR (LSR1 і LSR2) створюється окремий тракт LSP (LSP2), який охоплює LSR5, LSR6 і LSR7. Він, по суті, являє собою тунель між цими двома LSR. Мітки в цьому LSP відрізняються від міток, які LSR створили для LSP1. Це справедливо і для LSR3 і LSR4, так само як і для LSR, що знаходяться між ними. Для цього останнього сегмента створюється тракт LSP3. Для досягнення цього результату, тобто для передачі пакета через два мережевих сегмента, використовується концепція стека міток.

Оскільки пакет повинен слідувати через LSP1, LSP2 і LSP3, він буде переносити одночасно дві окремі мітки. Пари, які використовуються для кожного сегмента такі: для першого сегмента - мітка для LSP1 і LSP2, для

другого сегмента - мітка для LSP1 і LSP3. Коли пакет залишає першу мережу і приймається граничним маршрутизатором LSR3, той видаляє мітку для LSP2 і замінює її на мітку для LSP3, замінюючи при цьому мітку LSP1 всередині пакету на мітку наступного пересилання. Маршрутизатор LSR4 видаляє обидві мітки перед відправкою пакету адресату.

2.2 Порівняльний аналіз тунелів MPLS та звичайних тунелів

Тунелі MPLS дозволяють передавати дані будь-якого протоколу вищого рівня (наприклад, IP, IPX, кадри Frame Relay, осередки ATM), так як вміст пакетів вздовж усього шляху проходження пакету залишається незмінним, а змінюються лише мітки. На відміну від них, тунелі IPSec підтримують передачу даних тільки протоколу IP, а протоколи PPTP і L2TP дозволяють обмінюватися даними по протоколам IP, IPX або Net BEUI.

Безпека передачі даних в MPLS забезпечується за рахунок певної мережевої політики, яка забороняє приймати пакети, забезпечені знаками, і маршрутну інформацію VPN-IP від неперевірених джерел. Вона може бути підвищена використанням стандартних засобів аутентифікації і / або шифрування (наприклад, шифрування IPSec).

Для безпечної передачі даних в протокол IP Security включені певні процедури шифрування IP-пакетів, аутентифікації, забезпечення захисту і цілісності даних при транспортуванні, внаслідок чого, тунелі IPSec забезпечують надійну доставку інформаційного трафіку.

Протокол L2TP підтримує процедури аутентифікації, тунелювання інформаційного потоку, а PPTP, крім даних функцій, забезпечений і функціями шифрування.

Застосування міток MPLS дозволяє реалізувати прискорене просування пакетів по мережі провайдера. Транспорт MPLS не зчитує

заголовки пакетів, що транспортуються, тому що використовувана в цих пакетах адресація може носити приватний характер. Вміст пакетів не зчитується і при передачі IP-пакетів по протоколам IPSec, PPTP, L2TP. Однак, на відміну від MPLS традиційні протоколи тунелювання для транспортування IP-пакетів використовують традиційну IP-маршрутизацію.

При виборі шляху проходження пакету в MPLS враховуються різні параметри, що впливають на вибір маршруту. Спільна робота технології многопротокольної комутації і механізмів Traffic Engineering дозволяє для кожного тунелю LSP надати необхідний рівень якості обслуговування за рахунок процедури резервування ресурсів на кожному маршрутизаторі уздовж шляху проходження пакету. Крім цього, з'являється можливість відстежувати дійсний маршрут, що проходить через сформований тунель, можливість діагностики та адміністративного контролю тунелів LSP.

Різні тунелі, у відповідності до необхідного рівня QoS, між двома точками підтримує і протокол L2TP.

Технологія VPN IPSec не підтримує параметрів якості обслуговування встановленого з'єднання, а протокол PPTP підтримує один єдиний тунель між двома точками.

Не можна не відзначити і той факт, що весь трафік при використанні традиційних IP-тунелів слідує до адресата уздовж одного і того ж шляху. Технологія MPLS дозволяє контролювати потоки, що передаються по безлічі всіх наявних шляхів до адресата.

З точки зору багатоадресної розсилки варто відзначити, що жодна з розглянутих технологій її не підтримує, але щодо MPLS-TE, то вона знаходиться в розробці.

MPLS VPN може бути створена для підтримки критично важливих додатків на цілодобовій основі. У цьому випадку провайдер послуг визначає фіксований шлях на термін контракту з користувачем. У

випадках збою або відсутності пропускної здатності пріоритет віддається більш важливим потокам (з більш високим пріоритетом).

Одна з функцій MPLS - об'єднання віртуальних каналів, коли кілька тунелів MPLS об'єднуються для створення єдиного тунелю. Така структура поширює VPN на базі MPLS в мережі оператора на мережу всередині офісу і прямо до сервера або клієнта. При подібному розширенні VPN оператору може бути надана відповідальність з управління для забезпечення безперервного контролю за CoS з кінця в кінець.

2.3 Технологія VPN в мережі MPLS

На організацію приватних мереж впливають різноманітні фактори, одним із них являється вибір технології побудови VPN.

Поняття LSP-тунелів становить важливий аспект MPLS VPN, оскільки «приватний» в VPN на базі MPLS відноситься до фізичного поділу трафику між LSP-тунелями. В даний час, в області мереж MPLS VPN існують два основних напрямки: BGP/MPLS VPN та VPN з віртуальними маршрутизаторами на базі IP. Обидва ці напрямки відповідають загальній моделі MPLS VPN, представленої на рисунку 15.

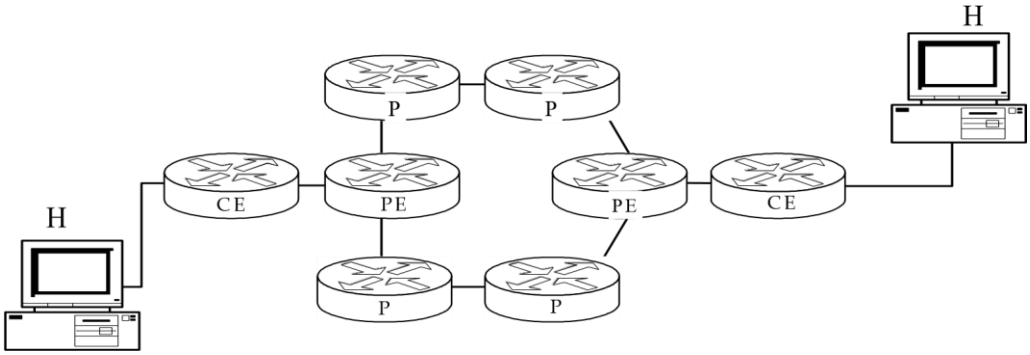


Рисунок 2.5 Еталонна модель MPLS VPN

Ядро мережі на рисунку 2.5 будується на базових маршрутизаторах MPLS, які називаються внутрішніми маршрутизаторами провайдера P і

взаємодіє з користувачем VPN не безпосередньо, а за допомогою з'єднання між граничним пристроєм маршрутизації замовника CE (Customer Edge router) і граничним пристроєм маршрутизації провайдера PE (Provider Edge router). CE можуть бути статично приєднані до PE провайдера через закріплені канали або можуть використовувати комутовані лінії зв'язку.

Обидва методи MPLS VPN подібні в створюваній провайдером послуги VPN функціональності. В одному методі протокол BGP використовується для створення спеціальних розширених адрес при передачі пакетів через ядро MPLS, а в іншому VR зберігають окремі таблиці шляхів MPLS для кожної VPN. Фактична ж реалізація цих двох методів абсолютно різна, а вибір методу - рішення провайдера послуг VPN на основі можливостей обладнання, ситуації з взаємодією мереж та інших факторів. Створено нову робочу групу IETF, названа Provider-Provisioned VPNs (PPVPNs), яка розробляє структуру і відповідні специфікації для цих двох типів мереж VPN.

Мережі MPLS / BGP-VPN

Модель MPLS / BGP VPN базується на розширеннях протоколу маршрутизації зовнішнього шлюзу BGP, що мають назву багатопротокольні розширення BGP і стосуються спеціальних розширених адрес. Ці адреси використовуються для обміну інформацією про доступність між маршрутизаторами PE тільки між членами однієї і тієї ж VPN. Кожен маршрутизатор PE в MPLS / BGP VPN підтримує окрему таблицю маршрутизації VRF (VPN Routing and Forwarding table). Така таблиця підтримується для кожного сайту, підключеного до PE маршрутизатора. Якщо IP-адреса пакета вказує на те, що його треба передати в сайт A, його шукають в таблиці (forwarding table) сайту A тільки в тому випадку, коли пакет прибуває з сайту, асоційованого з таблицею сайту A. Якщо сайт пов'язаний з декількома мережами VPN,

його таблиця VRF може включати дані про маршрути всіх цих мереж. Наприклад, сайт Ce1 належить мережі VPNA і VPNB. В цьому випадку таблиця VRF пристрої pe1, до якого приєднаний CE1, буде містити інформацію про маршрути мережі VPNA і VPNB. Іншими словами, на пристрої pe1 НЕ буде двох окремих таблиць VRF. Таблиці VRF на пристроях PE використовуються тільки для пакетів, що надходять з сайту, безпосередньо підключеного до пристрою PE. Вони не використовуються для маршрутизації пакетів, що надходять з інших маршрутизаторів, встановлених в магістралі сервіс-провайдера. В результаті, до однієї і тієї ж адреси в мережі можуть вести кілька маршрутів, тому що маршрут для передачі кожного пакета визначається в точці, через яку пакет потрапляє в магістраль. Дана модель дозволяє використовувати перекриття просторів приватних IP-адресацій різних підприємств. Основна мета цього типу реалізації MPLS VPN - дозволити провайдеру забезпечити створення необхідної замовнику конфігурацію VPN. Замовником в даному випадку може бути підприємство, група підприємств, яким потрібна «Екстранет», інший сервіс-провайдер або навіть інший провайдер VPN, який може використовувати цей MPLS-додаток з метою побудови мережі VPN своїм власним клієнтам.

Існує й інша модель організації MPLS VPN на 3 рівні. Вона базується на принципі освіти віртуальних маршрутизаторів. Ця модель не буде розглядатися через малу поширеность. Сьогодні, якщо мова йде про MPLS VPN L3, то розуміється MPLS / BGP-VPN.

Організація MPLS VPN

У загальному випадку, у клієнта може бути кілька територіально-відокремлених IP-мереж, кожна з яких, в свою чергу, може включати декілька підмереж, пов'язаних маршрутизаторами. Такі територіально ізольовані мережеві елементи корпоративної мережі прийнято називати сайтами. Сайти, що належать одному клієнту, обмінюються IP пакетами

через мережу провайдера і утворюють віртуальну приватну мережу цього клієнта. Як було зазначено під час обговорення рисунку 15, кожен сайт має один або кілька граничних призначених для користувача маршрутизаторів CE, з'єднаних з одним або більше граничними маршрутизаторами PE провайдера за допомогою каналів PPP, ATM, Ethernet, Frame Relay і т.п.

CE-маршрутизатори різних сайтів не обмінюються маршрутною інформацією безпосередньо і навіть можуть не знати один про одного. Адресні простори підмереж, що входять до складу VPN, можуть перекриватися, тобто унікальність адрес повинна дотримуватися тільки в межах конкретної підмережі. Цього вдається досягти перетворенням IP-адреси в VPN-IP-адреси і використанням протоколу MP-BGP для роботи з цими адресами.

Кожен PE-маршрутизатор повинен підтримувати стільки таблиць маршрутизації, скільки сайтів користувачів до нього приєднано, тобто на одному фізичному маршрутизаторі організується кілька віртуальних. Причому маршрутна інформація, що стосується конкретної VPN, міститься тільки в PE-маршрутизаторах, до яких під'єднані сайти даної VPN. Таким чином, вирішується проблема масштабування, яка неминуче виникає в разі наявності цієї інформації в усіх маршрутизаторах мережі оператора. Вважається, що CE-маршрутизатор відноситься до одного сайту, але сам сайт може належати до кількох VPN. До PE-маршрутизатора може бути підключено кілька CE-маршрутизаторів, що знаходяться в різних сайтах і навіть відносяться до різних VPN.

Реалізація VPN-MPLS

На рисунку 2.6 представлений фрагмент мережі VPN MPLS. Дана мережа об'єднує кілька віддалених користувачів і сайтів клієнтів через мережу провайдера MPLS. Об'єднані сайти і віддалені користувачі однієї компанії утворюють віртуальну приватну мережу даного підприємства.

Таким чином, на рисунку представлені дві VPN: підприємства А, що включає три сайти і віддалених користувачів і підприємства В, що включає два територіально розподілених філії.

В VPN MPLS мають місце два основних потоки трафіку:

- потік керування, що використовується для розповсюдження маршруту VPN і встановлення шляху комутації міток LSP.
- потік даних, що використовується для просування інформаційного потоку.

В свою чергу, потік керування складається з двух субпотоків:

- Перший відповідає за обмін маршрутною інформацією між PE та CE на межі магістралі постачальника послуг та між маршрутизаторами PE через магістраль провайдера.
- Другий субпотік відповідає за встановлення шляху LSP між маршрутизаторами PE через магістраль постачальника послуг.

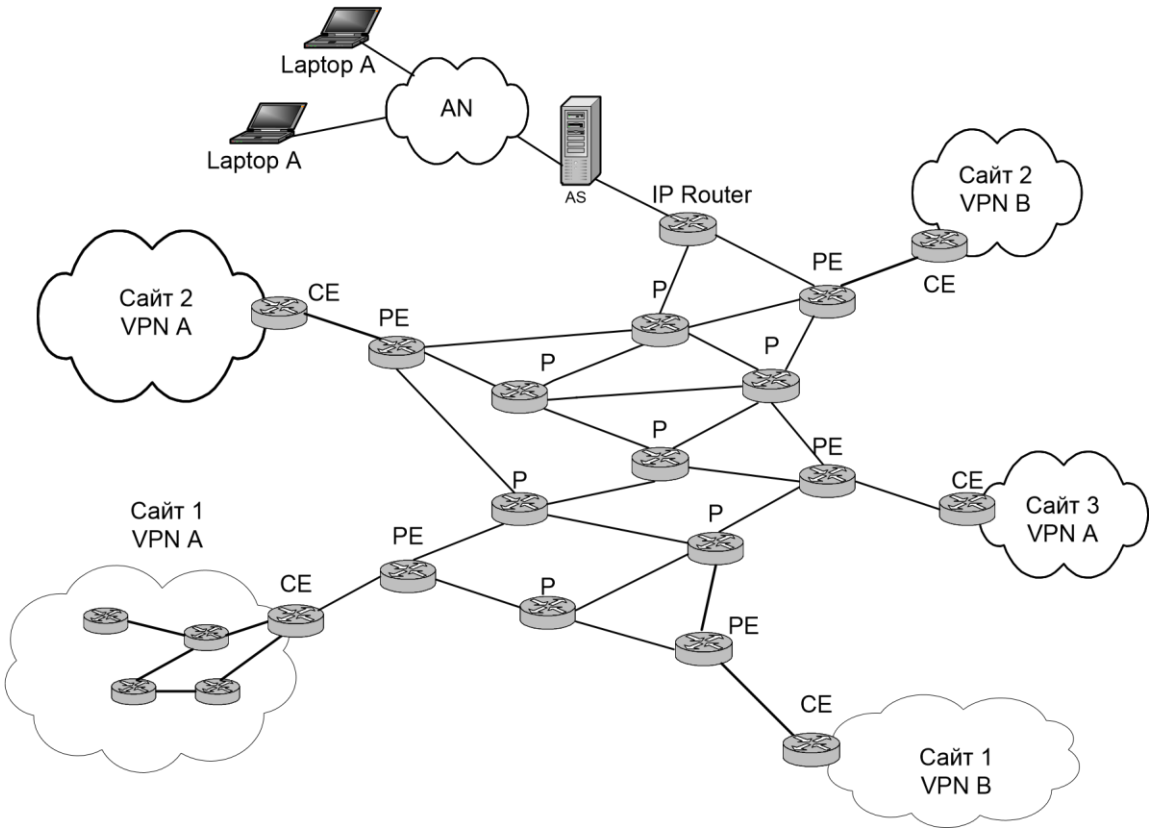


Рисунок 2.6 Віртуальна приватна мережа на базі технології MPLS

2.4 Огляд принципів роботи VPLS

VPLS - нова технологія і одночасно - послуга, яка може надаватися великій кількості корпоративних замовників і забезпечувати значні прибутки операторам. Послуга полягає в об'єднанні двох і більше віддалених офісів клієнта в єдину високошвидкісну і захищену мережу обміну інформацією.

Основу концепції VPLS становить ідея передачі пакетів Ethernet з мережі замовника (включаючи інформацію про внутрішні VLAN) по операторській мережі «прозорим» чином абсолютно без змін. Для цього пакети інкапсулюються за технологією MPLS, що забезпечує створення тунелів в мережі оператора зв'язку, які є незалежними від призначеного для користувача трафіку. Для реалізації цього завдання мережа оператора

повинна бути високонадійною, підтримувати новітні механізми відмовостійкості, такі як механізм сполучного дерева (Rapid Spanning Tree), що забезпечують найвищі гарантії доставки пакетів за призначенням, також механізми підтримки якості послуг. Замовникам не потрібно підключатися до IP-мережі оператора і налаштовувати складні протоколи IP-маршрутизації: вони використовують прості з'єднання Ethernet, які дозволяють працювати з набагато більшим числом різних мережевих архітектур і топологій.

VPLS особливо ефективна в умовах динамічного розвивитку ринку, де прибуток є найважливішим завданням. Замість встановлення дорогих маршрутизаторів і обладнання для IP-тунелювання, для побудови мережі доступу та операторської мережі можуть бути використані звичайні комутатори Ethernet, що забезпечує надання високошвидкісних сервісів при менших витратах. Оператори можуть скористатися наявними можливостями класифікації трафіку для надання послуг, що вимагають високого пріоритету, наприклад передача голосу по IP.

VPLS використовує стандарти IEEE 802.1q і MPLS Martini для інкапсуляції пакетів і їх транспорту, також сигналізація VPLS описана ще в ряді документів IETF.

На вході в мережу оператора, зазвичай в приміщенні замовника, комутатор Ethernet інкапсулює пакети локальної мережі в пакети з тегами 802.1q VLAN, навіть якщо замовник вже використовує VLAN. Цей процес, званий VMAN, додає до пакету додатковий тег VLAN, що дозволяє ідентифікувати приналежність даного пакета конкретного замовника. Вихідний тег, що описує приналежність пакета до однієї з внутрішніх VLAN в мережі замовника, залишається на місці і відновлюється на виході з операторської мережі. Всередині операторської мережі робота VPLS може здійснюватися двома основними способами. Якщо абонентів небагато (менше 4 тис.), теги VMAN можуть без змін

використовуватися для організації з'єднань. При більшій кількості абонентів (тисячах і десятках тисяч) мережу необхідно конфігурувати для застосування інкапсуляції MPLS, яка поміщає в пакети мітки, що дозволяють визначити їх походження і способи пересилання всередині мережі оператора. Незалежно від архітектури мережі оператора на виході з мережі пакет замовника відновлюється в своєму початковому вигляді, включаючи можливу наявність тега VLAN. Це дає замовнику можливість бути повністю незалежним від конфігурації мережі оператора, що є найважливішою функцією будь-якої послуги зі створення віртуальних приватних мереж.

При використанні VPLS допускаються з'єднання типу «точка-точка» і багатоточкові конфігурації. В останньому випадку обладнання вивчає розташування різних пристроїв в мережі і побудова відповідних таблиць для правильної пересилання пакетів між підключеними точками. З цією метою операторська мережу повинна забезпечувати надання гарантованої смуги пропускання і захист від перевантажень і заторів трафіку. Для вирішення цієї проблеми існують механізм класифікації трафіку Ethernet. При його застосуванні оператор може управляти виділеною смугою пропускання з високим рівнем контролю над реальною швидкістю проходження пакетів в мережі. Крім того, для забезпечення роботи додатків, що вимагають найвищого пріоритету для їх трафіку, він може використовувати класифікацію і додаткові можливості MPLS.

VPLS надає багатоточкові послуги Ethernet. VPLS може поєднати велику кількість областей і забезпечити з'єднання між численними сайтами так, немов ці сайти належати одному приватному сегменту локальної мережі Ethernet. У той час як для здійснення багатоточкового Ethernet з'єднання провайдер використовує базується на комутаторах Ethernet архітектуру, для побудови VPLS використовується масштабована структура мережі IP / MPLS. З точки зору провайдера, використання

маршрутних протоколів і процедур маршрутизації IP / MPLS замість протоколу сполучного дерева (Spanning Tree Protocol) і міток MPLS замість VLAN IDs (ідентифікаторів VLAN), а також використання різних служб провайдера веде до значного поліпшення масштабованості VPLS.

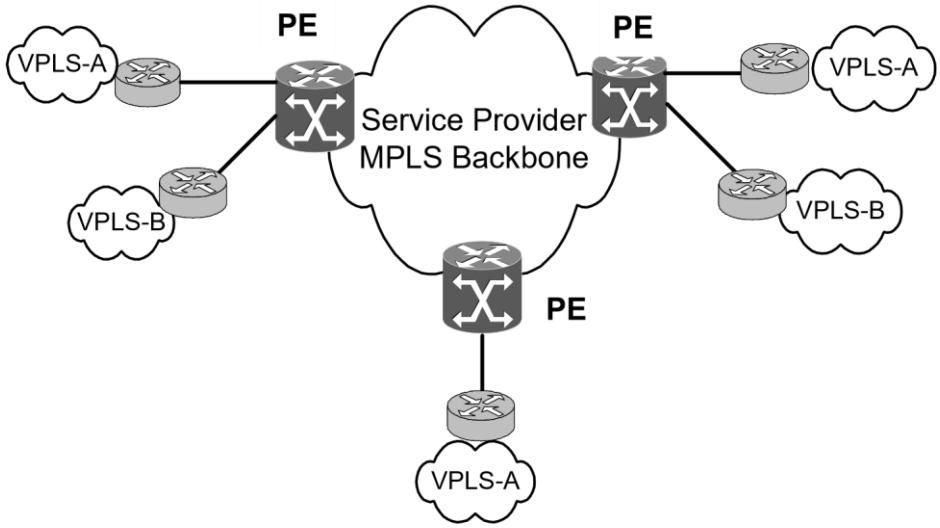


Рисунок 2.7 Приклад мережі VPLS

Кожен маршрутизатор провайдера PE (Provider Edge), розташований на межі IP / MPLS мережі, має особливі якості VPLS, визначеними стандартами IETF. Кожному підприємству, що бажає використовувати прозорі служби Ethernet, оператор виділяє домен VPLS. Кожен такий домен може розглядатися як приватна мережа Ethernet, яку провайдер реалізує в своїй мережі, а кожен пов'язаний з філією маршрутизатор створює «екземпляр VPLS». Кожен VPLS домен складається з певної кількості PE, що з'єднують екземпляри VPLS, що знаходяться в цьому певному VPLS домені, між собою. Спростимо ситуацію, припустимо, що є тільки один VPLS домен для якогось підприємства і на один екземпляр VPLS доводиться один PE, що з'єднує сайти, які належать цьому підприємству. Насамперед в домені VPLS провайдерської мережі для всіх примірників VPLS, необхідно створити повний набір шляхів комутації по

мітках (LSP). Залежно від реалізації, VPLS витрати на LSP при додаванні нових екземплярів VPLS можуть виявитися більш-менш значними.

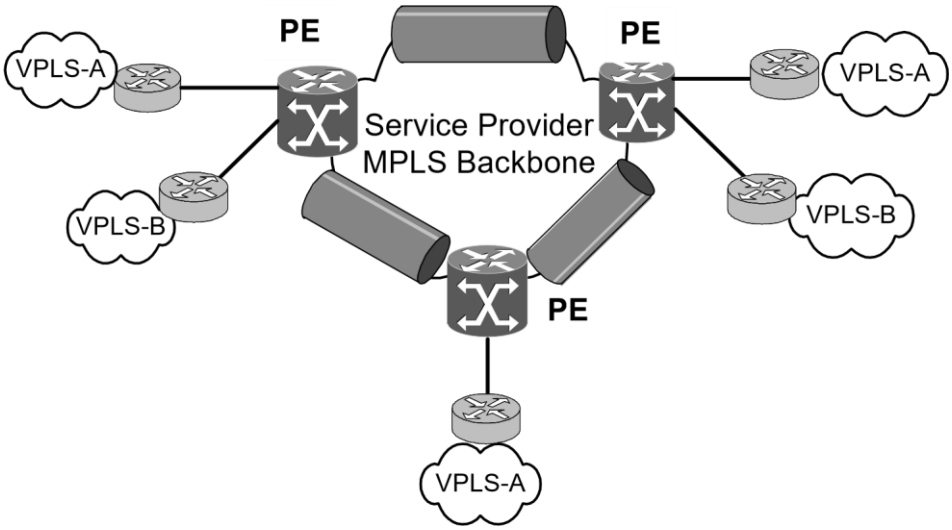


Рисунок 2.8 Повний набір шляхів комутації міток (LSP) між PE

Для організації необхідної кількості зовнішніх тунелів для PE використовується розширений метод виявлення сусідів MPLS, тобто спрямовані повідомлення Hello, що передаються по UDP. Потім встановлюється TCP сесія, і далі для створення LSP використовуються сигнальні повідомлення протоколу LDP.

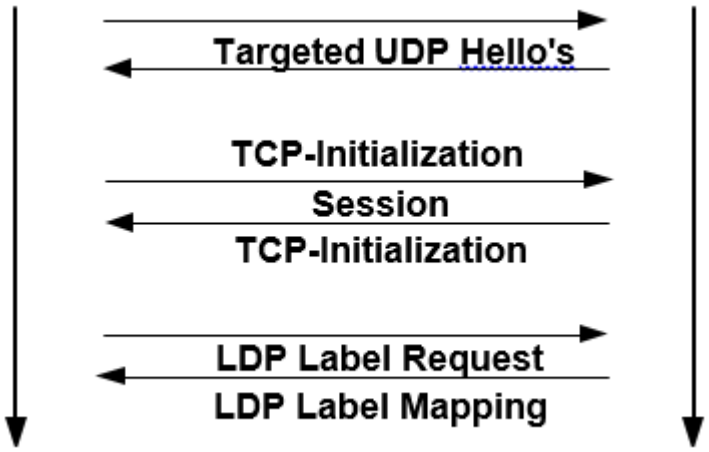


Рисунок 2.9 Використання протоколів UDP, TCP, LDP для створення LSP

Після того як повний набір LSP тунелів буде організований для всіх PE, екземпляр VPLS повинен призначити ідентифікатори VPLS і, отримавши сигнал від кожного PE, повідомити йому ідентифікатор VPLS Virtual Circuit Label або VC Labels. Для встановлення VPLS або VC-ID тунелів кожен PE ініціює спрямовану LDP сесію з кожним PE в екземплярі VPLS, щоб організувати два віртуальних канали (тому що віртуальні канали як і тунелі односпрямовані, то, відповідно, організовується один віртуальний канал в одному тунелі і другий віртуальний канал в зворотному напрямку в іншому тунелі) - VC або VPLS LSP, всередині зовнішнього тунелю LSP.

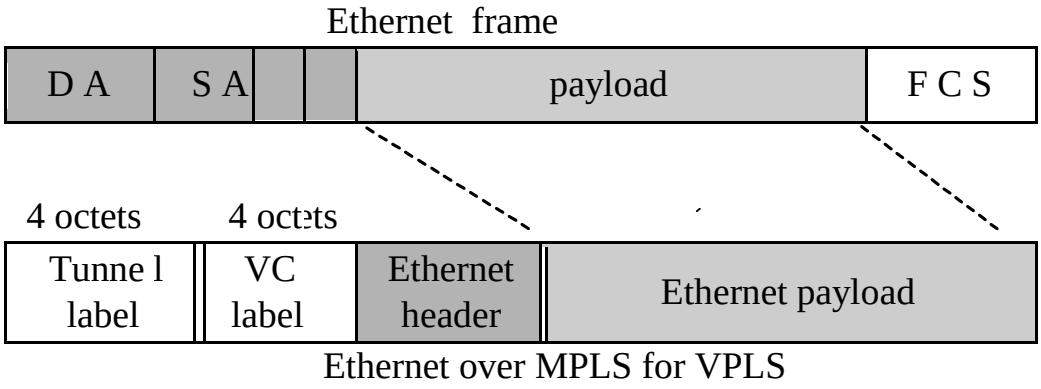
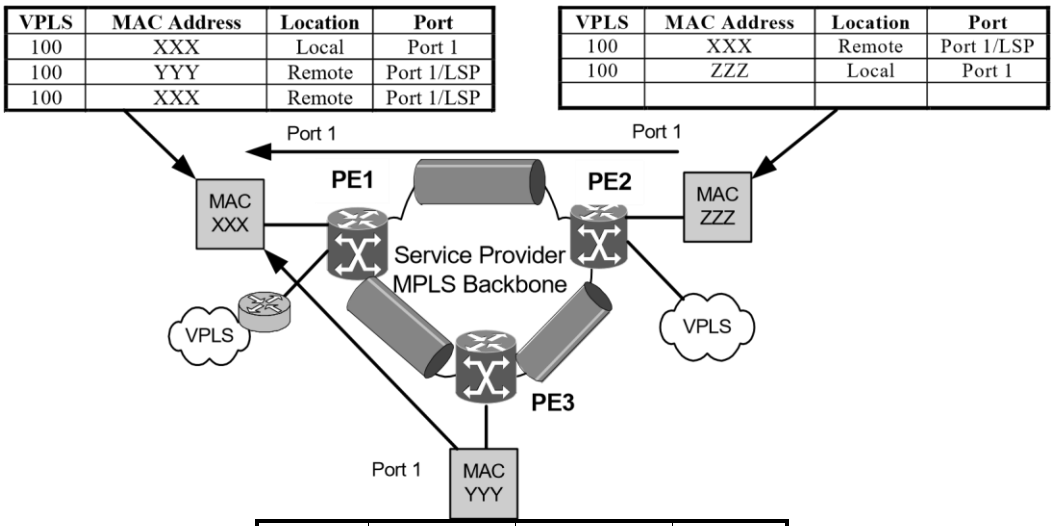


Рисунок 2.10 MPLS VPLS Label Stacking

Якщо побудова зв'язкової мережі LSP закінчилася, то екземпляри VPLS можуть приймати кадри Ethernet від будь-якої філії і в залежності від MAC-адреси передавати далі по відповідним LSP. Це можливо завдяки тому, що VPLS дозволяє PE маршрутизаторам працювати в якості «навченого» моста, тобто для кожного екземпляра VPLS кожен PE має таблицю MAC-адресу. Основними функціями VPLS моста є: «Навчання» і видалення MAC-адрес, передача невідомого трафіку, дублювання і многоточкова або широкомовлення невідомих пакетів. «Навчання» VPLS

мостів MAC-адресами відбувається також, як і «навчання» мостів Ethernet. А саме, MAC-адреса XXX надсилається широкомовно, як ARP-запит. Пристрої запам'ятовують цей MAC-адреса і асоціюють його з конкретним LSP.



VPLS	MAC Address	Location	Port
100	XXX	Remote	Port 1/LSP
100	YYY	Local	Port 1

Рисунок 2.11 «Навчання» MAC-адресам

PE1 запам'ятовує, що VPLS 100 має MAC-адреса XXX, що належить порту 1. Коли PE2 і PE3 широкомовно отримують запит, вони фіксують у себе MAC-адреси XXX і асоціюють його з LSP, який веде до PE1. Далі коли з MAC-адреси ZZZ надсилається відповідь на адресу XXX, PE2 закріплює за адресою ZZZ у себе порт 1, а PE1 запам'ятовує, що ZZZ належить PE2 віддалено і асоціює його з LSP, що зв'язує PE1 і PE2. Теж саме відбувається, коли надсилається відповідь з адреси YYY на адресу

XXX, тобто PE3 локально прикріплює до YYY порт 1, а PE1 - віддалено і асоціює цю адресу з LSP, що йде від нього до PE3.

Іншими словами, у кожного примірника VPLS є PE маршрутизатор, якому надається таблиця MAC-адрес, яка заповнюється в процесі відстеження MAC-адрес або процесі «навчання», коли Ethernet кадри надходять на спеціальний фізичний або логічний порт, тобто по цій таблиці маршрутизатор перевіряє і розпізнає кадри, що надходять на порт Ethernet. Таким же чином працюють і комутатори Ethernet сьогодні. Після надходження кадру на порт з боку підприємства маршрутизатор звіряє MAC-адресу місця призначення з таблицею і без змін направляє кадр на LSP або далі до певного граничного маршрутизатора. Якщо цієї MAC-адреси немає в таблиці, Ethernet кадр дублюється і розсилається на всі логічні порти, пов'язані з цим екземпляром VPLS, за винятком порту доступу, куди цей кадр тільки що прийшов (лавинна маршрутизація). Якщо граничний маршрутизатор отримує інформацію про призначення адреси на особливий порт, він оновлює таблицю. Як і в комутаторі, MAC-адреса, що довгий час не використовувалася, застаріває і в цілях збереження компактності таблиці MAC-адрес видаляється.

Існує дві лідируючих пропозиції, що в даний час обговорюються в IETF, які претендують на те, щоб стати основними підходами побудови VPLS. Перший стандарт - це draft-ietf-ppvpn-vpls-ldp (VPLS LDP), який будемо називати «стандарт Kompella», запропонований Кірееті Компелла. Другий - draft-ietf-ppvpn-vpls-bgp (VPLS BGP), який будемо називати «стандарт Lasserre-Kompella», запропонований Марком Лассерром і Вахом Компелла.

Розглянемо обидва стандарти і порівняємо за наступними критеріями:

- Ефективність розповсюдження сигнальної інформації.
- Ефективність розподіленням міток.

- Пошук пристроїв, що взаємодіють в рамках VPLS PE.
- Масштабованість.
- Наявність інструментарію адміністрування та налагодження.

Можливість організації VPLS на мережі декількох взаємодіючих операторів.

2.5 Порівняння VPN-MPLS та VPLS

Вироблення критеріїв порівняння

Обидва підходи VPN-MPLS і VPLS реалізуються на базі MPLS / IP мережі, яка використовується для надання різноманітних послуг численним клієнтам. Так, в мережі може існувати кілька клієнтів VPN, які володіють великими обсягами конфіденційної внутрішньокорпоративної інформації, крім послуги VPN мережу використовується для організації численних сервісів, відповідно .в мережі крім клієнтів VPN є велика кількість інших користувачів, також мережа забезпечує доступ в Інтернет, що ще більше розширює коло можливих користувачів. Отже, постає питання захисту інформації, переданої через MPLS / IP мережу. Відповідно, перший критерій, за яким будуть порівнюватися обидва підходи, - захищеність віртуальної приватної мережі замовника. Під захищеністю будемо розуміти запобігання крадіжки трафіку клієнтів VPN при передачі через мережу провайдера, запобігання доступу зловмисного користувача до ресурсів, розташованиш в сайтах клієнта, а також запобігання розкриття топології мережі користувача.

Іншою не менш важливою характеристикою операторської мережі є надійність. При наданні послуг провайдер повинен підтримувати необхідну якість обслуговування. Однією з основних складових підтримки необхідної якості обслуговування є забезпечення надійності

мережі провайдера. При розробці критерію надійності я не буду розглядати характеристики конкретного обладнання, тому що моїм завданням є порівняння технологій VPN-MPLS і VPLS, а не огляд існуючого обладнання. З точки зору мережевих технологій, під надійністю будемо розуміти можливість мережі по організації резервних каналів, по реконфігурації, тобто реакція мережі на виникнення різних аварійних ситуацій.

Клієнтські мережі можуть бути побудовані з використанням різних технологій і мережевих протоколів, наприклад протоколів IPX, SNA, технологій ATM, FR. Отже, технологія об'єднання мереж повинна мати властивість мультипротокольності, яке означає можливість мережі щодо забезпечення прозорої передачі призначених для користувача даних різного формату.

Для того, щоб мати можливість розвиватися згідно з вимогами сучасного ринку технологія, повинна забезпечувати масштабованість, побудованої на базі неї мережі. Розглянемо масштабованість як з точки зору клієнта, так і з точки зору оператора. З точки зору клієнта, мережа повинна забезпечувати можливість росту компанії клієнта, а отже організацію нових сайтів. З боку оператора, мережа теж повинна бути масштабованою, тому що розширюється оператор як компанія, було 10 клієнтів стало 110, відповідно повинна забезпечуватися можливість збільшення клієнтської бази. Також оператор може розширювати географічно область дії своєї мережі. Останнім часом широкосмугові послуги стають все більш популярні і затребувані в корпоративному секторі, і саме великі компанії, як правило, є основними замовниками нових послуг, так як корпоративний клієнт може запросити розширення смуги пропускання для своїх віртуальних приватних мереж. Тому масштабованість є важливим критерієм вибору технології. Під масштабованістю будемо мати на увазі здатність мережі оператора до

географічного розширення, збільшення клієнтської бази та нарощування потужності мережі.

Успіх провайдера сильно залежить від того, наскільки повно він зможе задовольнити запити клієнта. Тому гнучкість в підтримці різних мережевих топологій дозволить задовольнити ці запити оптимальним чином. Під підтримкою різних топологій зв'язності будемо розглядати можливість позначених підходів підтримувати такі мережеві топології зв'язності: точка-точка, hub-and-spoke, полносвязная топологія, частково зв'язкова і перекриття VPN.

Порівнювати технології можна буде, якщо перед нами стоїть проблема вибору, яка виникає, коли стоїть завдання побудови мережі на основі нової технології. Відповідно важливим фактором, що впливає на вибір тієї чи іншої технології, є складність її впровадження оператором. Під складністю впровадження технології будемо розуміти складність створення нової мережевої інфраструктури і складність адаптації існуючої мережевої інфраструктури оператора для реалізації технології.

Після створення мережевої інфраструктури для надання послуг віртуальних приватних мереж необхідно здійснювати адміністрування з метою надання послуг конкретним замовникам. Чим складніше механізм адміністрування, тим більше тимчасових витрат він зажадає від персоналу і відповідно більш високої кваліфікації обслуговуючого персоналу. Отже, більша ймовірність помилки на стадії організації надання послуги. Тому одним із критеріїв, яким слід керуватися при виборі технології, є складність організації надання послуги, під цим критерієм будемо розуміти наступне - конфігурацію пристроїв мережі для надання послуг VPN новому клієнтові або включення в VPN нових елементів мережі клієнта.

Після створення інфраструктури та підключення клієнта необхідно керувати віртуальною приватною мережею клієнта і підтримувати її в

працездатному стані. Під критерієм «керування і підтримка» будемо мати на увазі керування конфігурацією створеної віртуальної приватної мережі та усунення виникаючих несправностей. Від простоти і функціональності засобів керування мережею безпосередньо залежать такі характеристики як надання послуги, як якість і гнучкість надання послуги, тобто швидка зміна смуги пропускання на вимогу клієнта і т.д.

Під економічним критерієм будемо розуміти відносну потенційну економічну ефективність двох підходів. В рамках цього, економічну ефективність доцільно розділити на клієнтську і провайдерскую. Цей критерій для клієнта буде визначатися потенційними витратами на використання цієї послуги, а для провайдера буде визначатися його витратами на організацію послуги.

Порівняння VPN-MPLS та VPLS

Говорячи про захищеність інформації, що забезпечується VPN-MPLS і VPLS можна знайти багато спільного. Оскільки обидві технології побудовані на базі MPLS, при передачі трафіку через мережу провайдера організовуються тунелі, що в свою чергу ускладнює процес перенаправлення трафіку зловмисним користувачем. Обидві технології передбачають, що IP-заголовок не аналізується в мережі провайдера, тобто в таблицях маршрутизації ядра мережі провайдера немає інформації про клієнтські мережі, що дозволяє захистити топологію клієнтської мережі. VPN-MPLS для забезпечення безпеки використовує протокол IPSec. Протокол IPSec забезпечує захист на мережевому рівні і вимагає підтримки стандарту IPSec тільки сполучених між собою пристроїв по обидві сторони з'єднання. Усі інші пристрої, розташовані між ними, просто передають трафік IP. IPSec охоплює кілька абсолютно різних областей, в число яких входять аутентифікація, шифрування і управління ключами захисту. У забезпеченні безпеки в мережах VPN-MPLS велику роль відіграє протокол BGP. BGP присвоює унікальний параметр RD

логічним портам. Значення параметра RD невідомі кінцевим користувачам, і тому вони не можуть отримати доступ до цієї мережі через інший порт і перехопити чужий потік даних. BGP поширює таблиці FIB з інформацією про VPN тільки учасникам даної VPN, тим самим логічно розділяючи трафік і забезпечуючи захист передачі даних. Саме провайдер, а не замовник, надає порти певної VPN під час її формування. У мережі провайдера кожен пакет асоційований з RD, і тому спроби перехоплення пакету або потоку трафіку не можуть привести до прориву хакера в VPN. VPLS забезпечує прозору передачу трафіку, отже може використовувати різні методи шифрування. Отже, в силу своїх особливостей і спеціальних механізмів обидві технології і VPN-MPLS і VPLS забезпечують досить високий рівень захищеності.

Забезпечення надійності в мережі VPN-MPLS організовується за допомогою MPLS-TE і стандартними засобами MPLS Fast Reroute, а також можливостями протоколу BGP. MPLS-TE передбачає можливість автоматичного реконфігурування TE-тунелю при виникненні несправності зі збереженням характеристик цього тунелю. Під засобами MPLS Fast Reroute розуміється захист ланки даних резервним тунелем з локальним прийняттям рішення про перенаправлення трафіку. VPLS працює на базі протоколу LDP, який не має механізмів виявлення петель, швидкого реконфігурування мережі, відмовостійкості і т.д. При забезпеченні надійності, технологія VPLS в клієнтській мережі використовує Ethernet рішення, зокрема протокол STP, в мережі провайдера прийнято використовувати рішення MPLS / IP. STP - протокол сполучного дерева, який покликаний виявляти і усувати петлі при довільній топології LAN з діаметром мережі, що не перевищує 7 поспіль мостів. Також, STP здійснює резервування трактів і відновлення мережі в разі виникнення несправності. RSTP - модифікація STP (rapid STP),

швидше реконфігурує мережу, ніж STP, в мережах малого діаметра. Нарівні з протоколом STP може використовуватися протокол VRRP (Virtual Router Redundancy Protocol). При виході з ладу маршрутизатора на кілька хвилин може перериватися передача та обробка трафіку клієнтської мережі. VRRP покликаний усунути настільки тривалу перерву зв'язку шляхом заміни фізичного маршрутизатора за замовчуванням віртуальним маршрутизатором за замовчуванням (логічним), що включає в себе кілька фізичних маршрутизаторів. Таким чином, ці маршрутизатори дублюють один одного, при нормальному функціонуванні мережі вони працюють в режимі поділу навантаження, наприклад з декількома пристроями користувача. В аварійному режимі, справний маршрутизатор бере на себе все навантаження. Спочатку віртуальні приватні мережі побудовані на базі VPN-MPLS вважалися більш надійними, ніж мережі, побудовані на базі VPLS в силу того, що технологія VPN-MPLS ґрунтується на протоколі BGP. Для підвищення надійності мереж VPLS технологія передбачає використання спеціальних протоколів і механізмів, що ставить її в один ряд з технологією VPN-MPLS по забезпеченню надійності.

Порівнюючи обидва підходи по критерію мультіпрокольность, стає очевидно, що VPN-MPLS передбачає передачу тільки IP-трафіку. Підхід же VPLS дозволяє працювати з будь-яким протоколом третього рівня і передавати будь-які пакети, що надходять з мережі клієнта: IPv4, IPv6, IPX, DECNet, OSI і т.д. Багато клієнтів застосовують не тільки протокол IP, а й інші протоколи для створення своєї інфраструктури, а підхід VPLS не обмежує їх у виборі протоколу на відміну від VPN-MPLS. Сьогодні стає все більш популярним протокол IPv6, і багато організацій вже впроваджують його і в найближчому майбутньому збираються широко його використовувати. Для продовження взаємодії такого роду організацій з мережами VPN-MPLS потрібно поліпшення існуючого стандарту, а саме створення адресного простору VPN-IPv6, а також

розширення можливостей маршрутизаторів в мережі провайдера. Мережі ж VPLS можуть продовжувати обслуговувати подібні організації, навіть якщо мережа провайдера ще не запровадила IPv6 в своїй мережі.

Говорячи про масштабованость технологій VPN-MPLS і VPLS, можна знайти багато спільного. Обидві технології вважаються добре масштабованими в порівнянні зі схожими технологіями організації віртуальних приватних мереж, за рахунок того, що інформація про мережу клієнта на зберігається в маршрутизаторах ядра мережі, а зберігається лише на граничних маршутизаторах, які безпосередньо пов'язують мережу клієнта з мережею провайдера. Обмежуючим фактором масштабованості для обох підходів буде максимальне число LSP або VC, яке зможе підтримувати даний LSR. Іншим обмежувальним чинником, знову таки, для обох підходів буде максимальний розмір даних конфігурацій, які можуть зберігатися на одному PE маршрутизаторі, тому що дані конфігурації містять всю інформацію, що стосується віртуальної приватної мережі замовника. В технології VPN-MPLS дані конфігурації містять інформацію для VRF, RD, віддалених областей, фільтрації маршрутів. В технології VPLS дані конфігурації містять інформацію для VPN, пов'язаних з різними PE і для портів, асоційованих з VPN користувача. Використання автоматичного виявлення в сукупності з рішеннями VPLS зменшує обсяг інформації конфігурації для VPN, пов'язаних з різними PE і отже зменшує ступінь впливу розмірів даних конфігурації на масштабованість. Для VPN-MPLS кількість маршрутів, яке може зберігатися на одному PE також накладає певні обмеження на можливості масштабованості мережі, тому що PE маршрутизатор зберігає маршрути для всіх віртуальних приватних мереж, з якими він пов'язаний. Щоб пом'якшити вплив даного чинника на можливість масштабованості, де можливо використовується об'єднання маршрутів. Для VPLS максимальне число forwarding table entries, підтримуваних одним PE

маршрутизатором, вносить деякі обмеження. PE маршрутизатор створює entries для того, щоб мати можливість здійснювати функції комутації. Зменшення впливу цього фактора вимагає, щоб РЄ пристрої були маршрутизаторами і / або обмежувалося число (MAC) entries, створюваних для кожної віртуальної приватної мережі. Це допомагає користувальницькій VPN уникнути перевантаження PE великим числом MAC-адрес джерела. Отже, існують деякі обмеження мастштабованості технологій VPN-MPLS і VPLS, проте існує також і ряд способів зменшення впливу цих факторів. Тому технології VPN-MPLS і VPLS вважаються добре масштабованими. Для VPLS з метою підвищення спроможності масштабованості розроблена ієрархічна VPLS (HVPLS).

Підтримка топологій зв’язності

Підхід VPN-MPLS найбільш прийнятний для реалізації наступних топологій зв'язності: точка-точка, повнозв’язна і перекриття VPN, тому що вони прозорі для PE-пристроїв. Однак, VPN-MPLS, подолавши певні труднощі, може працювати з топологиями hub-and-spoke і частково зв'язковий. Для роботи VPLS більш підходять топології точка-точка, повнозв’язна, частково зв'язкова, hub-and-spoke. Очевидно, що hub-and-spoke і частково зв'язкова топологія легше реалізується VPLS, за рахунок використання VC, ніж VPN-MPLS, тому що BGP здійснює контроль маршрутів. VPLS також може використовувати топологію перекриття VPN, однак це вимагатиме залучення PE-пристроїв сайту, де це перекриття відбувається: PE має контролювати який маршрут співвідноситься з яким VPN, тобто при такій топології PE пристрої не є прозорими, як в разі VPN-MPLS. Завдяки своїм функціональним особливостям технологія VPN-MPLS краще реалізує одні топології зв'язності, а VPLS інші. Відповідно, в залежності від того, яка топологія зв'язності найбільш імпонує оператору вибирається та чи інша технологія.

Важкість впровадження

Для створення віртуальних приватних мереж на базі технології VPN-MPLS зазвичай потрібна наявність висококласних кінцевих маршрутизаторів LSR, здатних підтримувати численні маршрути і пересилання даних на граничний маршрутизатор провайдера PE. Також необхідно, щоб здійснювався рівноправний інформаційний обмін між цими маршрутизаторами. Якщо служби провайдера вже досить широко використовують протокол BGP по всій мережі, то в разі інтенсивного IP-трафіку доцільно використовувати VPN-MPLS, тому що це дозволить використовувати вже існуючі BGP з'єднання і LSP, вже організовані між PE для перенесення трафіку. Однак, при використанні існуючих BGP-з'єднань, варто внести деякі зміни в область, яка обслуговується одним відбивачем маршрутів для того, щоб відбивач маршрутів не вийшов із ладу через занадто велику кількостість маршрутів до різноманітних VPN. Якщо провайдер використовує конфедерацію, то ця проблема стає схожою на проблему inter провайдера, де VPN слід об'єднати безліч автономних систем. Схожа ситуація і з відбивачем маршрутів, провайдеру слід ретельно продумати, що має бути зроблено, щоб уникнути виникнення з'єднань маршрутизаторами і членами ASes, щоб не відбувалося переповнення маршрутами. Технологія VPLS вимагає більш простих в функціональному плані PE-маршрутизаторів і не вимагає наявності рівноправних BGP сесій, встановлених між PE. Служба провайдера, яка не ґрунтується на BGP або не схильна до побудови нових сервісів VPN на базі BGP, уникне тим самим багатьох складнощів, рішення технології VPLS можуть виявитися більш привабливими. Чи використовувати BGP для сигналізації між PE чи ні вирішує кожен провайдер для себе сам. У разі, якщо BGP вже впроваджений, подальше його використання обіцяє певні вигоди, наприклад, як уже згадувалося, наявність LSP з'єднань між PE для передачі трафіку. Як випливає з вищесказаного, технологія VPN-MPLS менш складна в адаптації до

існуючої мережевої інфраструктури оператора, якщо там використовується протокол BGP. А технологія VPLS є більш простий з точки зору впровадження оператором.

Важкість організації надання послуг

Складність організації надання послуги для технології VPN-MPLS полягає в організації процесу маршрутизації для кожної топології зв'язності віртуальної приватної мережі, необхідної замовником. Це означає створення VRF, які будуть містити всю інформацію про маршрути користувача і вибирати як призначати RD і Route Target Communities. Зауважимо, що служба провайдера повинна вирішити чи варто VRF підключати користувачів до певних інтерфейсів, тим самим розділяючи їх або варто зібрати маршрути до різних VPN, як в разі перекриття VPN. Також слід розподілити RD і Route Target Communities для надання послуг VPN. PE-маршрутизатори з'єднуються з сайтами користувачів, що змушує VPN конфігурувати необхідні VRF, RD і Route Targets і інше, що може знадобитися для роботи з певною топологією. Клієнтський маршрутизатор PE повинен володіти тими ж функціями, що і PE маршрутизатор провайдера, щоб мати можливість змінити маршрут, при необхідності. Організація надання послуги на базі технології VPLS дещо простіше. Кожному PE маршрутизатору, з'єднаному з віртуальною приватною мережею, необхідно мати інформацію про інших PE для встановлення VC із заданою VPN. Порт PE маршрутизатора, з'єднаний з сайтом користувача співвідноситься з конкретною VPN. Зауважимо, що використання автоматичного виявлення виключає необхідність детально конфігурувати PE, що мають відношення до тієї ж VPN.

Керування та підтримка

Керування віртуальною приватною мережею, побудованої на базі технології VPN-MPLS, полягає в тому, що при зміні конфігурації або рішенні проблем, що виникають при усуненні несправності, інженери

служби провайдера повинні вручну провести всі необхідні операції з BGP-сполуками, BGP-маршрутами до різних віддалених областях, їх розподіл і вибір PE, який буде здійснювати рівноправний інформаційний обмін з клієнтським PE- маршрутизатором і т.д. Як і в більшості масштабованих IP-мережах, область відбивача маршрутів або конфедерація з численними членами ASes можуть сприяти ускладненню вищезгаданого завдання. Робота з великим числом маршрутів, що відносяться до численних таблиць маршрутизації і пересилання, крім глобальної таблиці, звичайно, вимагає більше можливостей, ніж робота з однією таблицею. Нарешті, дані конфігурації, що знаходяться на PE-маршрутизаторі, розростуться до такої міри, що буде складно покрити неконфігуровану область. Підхід VPLS вирішує цю задачу простіше, тому що провайдер не зберігає ніякої інформації, пов'язаної з маршрутами клієнта, не контролює їх розподіл або обмін інформацією між різними клієнтськими PE-маршрутизаторами. Оскільки не використовується протокол BGP управління і усунення несправностей також спрощуються, інженери служби провайдера мають справу з VC, створюваних для VPN і портами, з'єднаними з конкретної VPN. На одному PE-маршрутизаторі інженери мають справу тільки з однією таблицею маршрутизації, незважаючи на те, що VFI таблиця MAC-адресами джерела в процесі навчання. Також як і у випадку VPN-MPLS, при сильному збільшенні обсягу даних конфігурації стає складніше розпізнавати неконфігуровані області мережі. Як вже говорилося раніше, використання автоматичного виявлення може істотно знизити обсяг даних конфігурації.

Економічний критерій

Порівнюючи вартість впровадження технологій, слід зазначити, що вартість розробки VPN-MPLS буде трохи вище, але все-таки вище, ніж рішення технології VPLS, за рахунок того, що підхід VPN-MPLS передбачає більш складні маршрутизатори, здатні підтримувати численні

VRF. Вартість управління і підтримки розглянутих підходів безпосередньо залежить від складності підходу. Очевидно, що VPN-MPLS буде мати більш високу вартість, за рахунок своєї складності, в порівнянні з VPLS. Складність підходу вимагає наявності деякого рівня застосовуваного обладнання, тобто обладнання, що задовольняє сучасні вимоги провайдера.

2.6 Висновки з розділу 2

MPLS стала основною магістральної технологією нового століття. Вона дозволяє ефективніше передавати великі об'єми трафіку в магістральних мережах і розглядається як основа для конвергенції послуг і фундамент для побудови мультисервісних мереж наступного покоління. Одна з функцій MPLS - об'єднання віртуальних каналів, коли кілька тунелів MPLS об'єднуються для створення єдиного тунелю. В даний час, в області мереж MPLS VPN існують два основних напрямки: BGP/MPLS VPN та VPN з віртуальними маршрутизаторами на базі IP. VPLS - нова технологія і одночасно - послуга, яка може надаватися великій кількості корпоративних замовників. Основу концепції VPLS становить ідея передачі пакетів Ethernet з мережі замовника по операторській мережі «прозорим» чином абсолютно без змін.

3 ОРГАНІЗАЦІЯ ВІРТУАЛЬНОЇ ПРИВАТНОЇ МЕРЕЖІ

3.1 Постановка задачі

Компанія-провайдер надає послугу організації мережі бізнес-клієнта з використанням транспортної технології MPLS для VPN з'єднання сайтів споживача через мережу провайдера.

Перед реалізацією нової пропозиції необхідно змоделювати та показати працездатність мережі. В моделі використані маршрутизатори Cisco 7200, Cisco 2691. Cisco 7200 використані у якості CE-маршрутизаторів, а Cisco 2691 – у якості PE-маршрутизаторів. Саме такий вибір було зроблено через те, що Cisco 7200 – це серія потужних маршрутизаторів, які ідеально підходять для мережі провайдера, а Cisco 2691 – недорогі маршрутизатори, що підтримують усі необхідні протоколи та підходять для більшості офісів (до 250 чол.), і з економічної точки зору їх вибір є більш доцільним.

Спочатку треба змоделювати мережу провайдера та мережу клієнта. Потім з використанням відповідних методик маршрутизації та переадресації трафіку зконфігурувати MPLS VPN між PE маршрутизаторами провайдера, до яких підключений клієнт. На моделі (Рисунок 21) R1, R2 та R3 представляють мережу провайдера, HQ – центральну точку, BRANCH – філії.

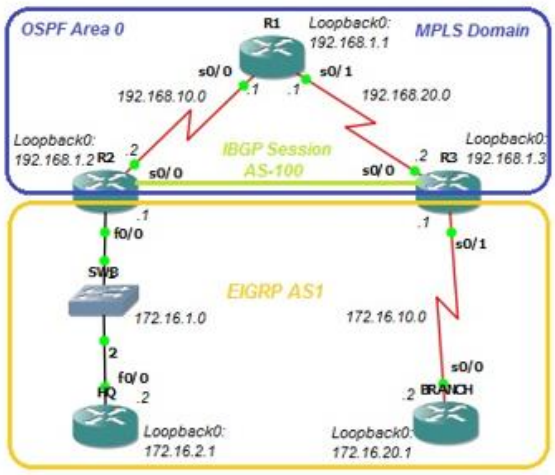


Рисунок 3.1 Модель організації бізнес-підключення

3.2 Конфігурування мережі

Конфігурування адресації

Спочатку необхідно розподілити адреси між усіма Loopback, Serial та Fast-Ethernet інтерфейсами , що показані на діаграмі та включити їх командою no shutdown на всіх фізичних інтерфейсах.

Перевірка підключень виконується командою ping з домену провайдера.

Виконуємо конфігурування мережі оператора та клієнтських сайтів HQ та BRANCH(код в додатку 2).

Конфігурування маршрутизації в домені провайдера

На мережі провайдера використовується OSPF як протокол маршрутизації. Тому необхідно виконати наступні дії:

- оголосити внутрішні loopback-інтерфейси та транзитні мережі, зконфігурувати OSPF для моделювання домену провайдера
- додати адреси всіх інтерфейсів, що анонсуються в головній мережі 192.168.0.0 в Area 0 процесу OSPF.

OSPF необхідно сконфігурувати лише на PE-роутерах R1, R2 та R3(код в додатку 2).

ORF сусідство має бути між R1 та R2 і між R2 та R3. Якщо OSPF не встановлено, необхідно перевірити налаштування інтерфейсів, налаштування OSPF та фізичні підключення.

Конфігурація MPLS в домені R

На всіх маршрутизаторах провайдера використовується інтерфейс Loopback 0 як ідентифікатор маршрутизатора router ID для Label Distribution Protocol (LDP). Інтерфейс loopback вибирається для кожного маршрутизатору автоматично, але доцільно задати значення ID, щоб вони не змінювалися під час зміни топології або перезавантаження маршрутизаторів. Для того, щоб задати loopback-інтерфейс як router ID для LDP, використовується команда mpls ldp router-id interface force в режимі глобальної конфігурації.

Для активації MPLS на фізичних інтерфейсах в MPLS-домені використовується команда mpls ip(код в додатку 2).

В результаті повинно з’явитися консольне повідомлення, що маршрутизатори з активованим MPLS стали сусідами через LDP. Перевірити, чи стали маршрутизатори сусідами можна командою show mpls ldp neighbor(код в додатку 2).

Конфігурування VRF

MPLS VPN є Layer 3 VPN, що дозволяє маршрутизацію пакетів через ядро MPLS. Цей тип VPN забезпечує клієнтам підключення до декількох сайтів через мережу провайдера. Провайдер має забезпечувати не тільки фізичне з'єднання, а й можливість динамічного маршруту між кінцевими точками VPN.

Важливо відзначити, що ні C, ні CE маршрутизаторам не потрібно ніяких спеціальних налаштувань. Для P маршрутизаторів потрібна тільки проста MPLS LDP конфігурація.

Кожен VRF використовує і підтримує свою власну інформаційну базу маршрутизації (RIB) і CiscoExpressForwarding (CEF).

Для активації CEF в режимі глобальної конфігурації застосовується команда ipcef на інтерфейсах, що пов'язані з VRF.

Для налаштування VRF на PE маршрутизаторах в режимі глобальної конфігурації застосовується команда ip vrf name на R1 та R3. В рядку конфігурації VRF створюється VRF з ім'ям «customer». Кожному VRF необхідно встановити route distinguisher та route target.

Налаштування маршруту Distinguisher (RD) 100:1 і routetarget (RT) 1:100 проводиться за допомогою команд rd ASN:nnand route-target{import | export | both} nn:nn. В даному випадку потрібно ключовим є слово both, тому що необхідно, щоб PE маршрутизатори імпортували і експортували з цієї VRF(код в додатку 2).

Команда vrf forwarding name, де name – ім'я конкретної VRF, задається на інтерфейсах маршрутизаторів R1 та R3 (PE-роутери, що стоять перед CE-роутерами). Також необхідно задати IP адреси(код в додатку).

На даному етапі вже має проходити пінг через лінки PE-CE. Але оскільки їх немає по замовчуванню в таблиці маршрутизації, необхідно використовувати команду ping vrf nameaddress. Для клієнта VRF є прозорою, тому при пінгуванні з C та CE маршрутизаторів можна використовувати традиційну команду ping(код в додатку 2).

Конфігурація EIGRPAS 1

Провайдер використовує BGPAS 100, а клієнт використовує BGPAS 1. Щоб зберегти конфігурацію логічно послідовною, треба використовувати номер AS 100 для EIGRP і BGP в мережі провайдера і номер 1 для EIGRP і BGP в мережі замовника. Тобто налаштовується EIGRPAS 1 на маршрутизаторах PE з глобальної конфігурації EIGRPAS 100.

На маршрутизаторах клієнта конфігурується EIGRPAS 1 для головної мережі 172.16.0.0 та відключається автоматичне

підсумування(код в додатку 2).

На маршрутизаторах PE конфігурація є більш складною. Кожен IGP має інший метод налаштування VRF. Для реалізації EIGRP для VRF необхідно запустити процес EIGRP по налаштуванню EIGRP AS 100. Якщо EIGRP використовується в якості IGP замість OSPF, необхідно налаштувати звітність мережі в цій точці(код в додатку 2).

Для налаштування EIGRP для конкретної VRF використовується команда address-familyipv4 vrfname, де name – ім'я VRF.

Хоча кожен VPN повинні бути логічно відокремлені від інших адрес IPv4 простору за допомогою VRF, цей поділ має поширюватися не тільки на таблицю маршрутизації, а й на протоколи маршрутизації. Команда address-family створює логічний сегмент протоколу маршрутизації і його маршруту для того, щоб відокремити його від інших наборів маршрутів. Використовуючи команду router eigrp 100 буде відокремлена автономна система EIGRP від усього домену EIGRP. Мережі, анонсовані через цю нову автономну систему, будуть введені в таблицю маршрутизації VRF, що пов'язана з ізольованою EIGRP AS. Важливо також зазначити, що ці мережі не будуть оголошені у будь-яким з сусідів EIGRP AS 100; вона повністю відділена від іншої частини домену EIGRP(код в додатку 2).

Перегляд таблиці маршрутизації по замовчуванню на PE маршрутизаторах виконується командою show ip route. PE маршрутизатори не мають головну мережу 172.16.0.0/16 в таблиці маршрутизації по замовчуванню. Відобразити таблицю маршрутизації VRF можна командою show ip route vrf name, де name – ім'я конкретної VRF(код в додатку 2).

Маршрутизатори R1 та HQ не мають в таблицях маршрутів для клієнта на R3 та BRANCH і навпаки.

Конфігурація BGP

Тепер, коли PE-маршрутизатори мають маршрути до CE-

маршрутизаторів через VRF таблиці, можна налаштовувати обмін інформацією між PE-маршрутизаторами через BGP. Спершу необхідно сконфігурувати BGP між R1 і R3 та між їх loopback-адресами. У нових версіях IOS синхронізація має бути відключена. Якщо синхронізація не відключена, для відключення синхронізації можна використати команду no synchronization(код в додатку 2).

Для конфігурування обміну маршрутима VPNv4 через BGP використовується команда address-familyvpnv4. Також необхідно оголосити сусідів BGP для даної сім'ї адрес за допомогою команди neighbor address activate. Оголошення сусідів для сім'ї адрес дозволяє BGP відправляти маршрути та отримувати маршрути від сусіда, використовуючи вказану сім'ю адрес. По замовчуванню сусіди активовані лише для IPv4.

RT є розширеними групами BGP, тому необхідно дозволити R2 і R3 відправляти стандартні та розширені групи через MP-BGP за допомогою команди neighbor address send-community both(код в додатку 2).

Отже, тепер потрібно налаштувати BGP перерозподіл EIGRP маршрутів в RIBVRF в протокол BGP, так щоб вони оголошувалися на віддаленому PE-маршрутизаторі. Відповідно до основної конфігурації BGP, вводиться інша адреса сім'ї, що пов'язана тільки з таблицею маршрутизації VRFcustomer. Перерозподіл EIGRP маршрутів, що пов'язані з цим VRF в BGP(код в додатку).

EIGRP, що містить VRF конфігурації з R1 і R3, налаштовується для перерозподілу маршрутів BGP, додається метрика з пропускною здатністю 64 Кбіт, 100 мкс, надійність 255/255, навантаження на 1/255, і MTU в 1500 байт(код в додатку 2).

На завершальному етапі необхідно дослідити маршрутизацію і форвардинг інформації, пов'язаної з маршрутом до 172.16.20.0/24. Потрібно переконатися, що маршрути анонсуються на віддалені

маршрутизатори PE. Використовується команда showiproutevrfname, щоб побачити RIBVRF(код в додатку 2).

Щоб побачити повний повну таблицю маршрутизації на CE, використовується команда show ip route(код в додатку 2).

Подивитись інформацію про маршрути BGP VPNv4 на R2 можна командою show bgp vpnv4 unicast all(код в додатку 2).

Для цього маршруту метрики (MED) в BGP є метрикою, що оголошується через EIGRP.

Переглянути більш детальну інформацію про конкретні префікса можна використовуючи команду show bgp vpnv4 unicastall ip-address. Інформація про MPLS мітки також включена.

R3 оголошує 172.16.20.0/24 префікс через BGP, а R2 отримує маршрут через BGPNLRI(код в додатку 2).

BGP передає інформацію про маршрути в NLRI як про розширені групи. Ці значення TLV вказує такі ознаки як: EIGRP тег, номер AS, пропускну здатність, затримку, надійності, навантаження, MTU і кількість хопів.

В MPLS мітці для маршруту BGP вище "Nolabel" на R1 означає, що R1 неоголошує мітку для мережі 172.16.20.0/24.

Переглянути список MPLS міток, які використовуються BGP можна за допомогою showbgpvpnv4 unicastalllabels(код в додатку 2).

Відображення атрибуту маршруту і той же префікс, 172.16.20.0/24, в

EIGRP таблиці топології на R1 виконується за допомогою команди show ip eigrp vrf customer topology ip-prefix/mask(код в додатку 2).

R1, P-маршрутизатор, він не має інформації про окремі маршрути в VRF таблиці на маршрутизаторах PE(код в додатку 2).

Пінг між CE маршрутизаторами для перевірки підключення через MPLS VPN(код в додатку 2).

MPLS має дві таблиці: LabelInformationBase (LIB) і

LabelForwardingInformationBase (LFIB). Як правило, LDP- allocated мітки оголошуються в LDP пірах. BGP- allocated мітки оголошуються в BGP пірах. BGP- allocated мітки будуть використовуватися BGP пірами, як MPLS мітки на пакетах, що призначені для цієї VPN мережі. BGP-allocated мітки мають значення тільки на вході і на виході маршрутизаторів. P-маршрутизатори, які не є BGP пірами з маршрутизаторами PE не побачать VPN мітку для мереж, анонсованих по BGP.

Коли BGP впізнає MPLS мітку, що використовується в якості мітки VPN, ця інформація заноситься в таблицю форвардингу CEF на вході PE. Показати форвардинг CEF для 172.16.20.0/24 на R2 можна командою show ip cef vrf name ip-address(код в додатку 2).

Для відображення оголошених міток R2 через LDP використовується команда show mpls ip binding(код в додатку 2).

CEF додає пакету мітку 20, а потім додається зовнішня мітка 16. Таблиця форвардингу CEF вирішує, який шлях буде використовуватися за замовчуванням RIB. Маршрут був встановлений в RIB на OSPF. Таким чином, вхідний PE накладає дві мітки в послідовності {16, 20}, як показано в таблиці CEF.

Оскільки вхідні пакети VPN з R1 інкапсулюються в MPLS кадри, R2 діє відповідно до директив в LFIB. R2 це передостанній хоп по мітці на шляху від R1 до loopback інтерфейсу R3, і тому використовується зовнішня MPLS мітка. Відобразити LFIB можна командою show mpls forwarding-table(код в додатку 2).

Для LFIB не має значення, чи є внутрішня мітка чи ні, він просто виконує операції, зазначені в стовпчику "tag or VC "(код в додатку 2).

Фінальна конфігурація кожного з маршрутизаторів приведена у додатку.

3.3 Висновки з розділу 3

Спочатку треба змоделювати мережу провайдера та мережу клієнта. Потім з використанням відповідних методик маршрутизації та переадресації трафіку зконфігурувати MPLS VPN між PE маршрутизаторами провайдера, до яких підключений клієнт.

ВИСНОВКИ

MPLS (Multiprotocol Label Switching) являється провідною технологією нашого часу. В дипломній роботі, яка була присвячена розробці функціональної моделі ділянки VPN на основі тунелів MPLS, були розглянуті сучасні технології побудови віртуальних приватних мереж, проведено порівняльний аналіз тунелів, побудованих на базі технології многопротокольной комутації на основі міток. В результаті проведеного аналізу можна зробити висновок про те, що технологія VPN MPLS на сьогоднішній день є провідною технологією побудови віртуальних приватних мереж. Вона володіє широкою масштабністю, гнучкістю, що не накладає жодних обмежень на протоколи вищого рівня, а застосування міток для комутації в мережі провайдера MPLS дозволяє реалізувати прискорену передачу трафіку по магістральній мережі. Використання розробленої в даній роботі функціональної моделі ділянки VPN дозволяє продовжити більш детальне розгляд даного варіанти організації віртуальних приватних мереж.

СПИСОК ЛІТЕРАТУРИ

1. Али С. Потоковая модель динамической балансировки очередей в MPLS-сети с поддержкой traffic engineering queues / С. Али, А.В. Симоненко // Проблемы телекоммуникаций. — 2010. — № 1. — с. 59–67.
2. Бараш Л. Виртуальные частные сети на базе MPLS / Леонид Бараш // Компьютерное Обозрение. — 2004. — № 17. — с. 14–16.
3. Cisco Systems: документация [Электронный ресурс]. Режим доступа: http://www.cisco.com/en/US/docs .
4. Cisco Systems: конфигурации [Электронный ресурс]. Режим доступа: http://www.cisco-conf.ru/ .
5. Гольдштейн А.Б. Технология и протоколы MPLS / А.Б. Гольдштейн, Б.С. Гольдштейн. — СПб. : БХВ – Санкт-Петербург, 2005. — 304 с.
6. Олвейн В. Структура и реализация современной технологии MPLS. Руководство Cisco / Вивек Олвейн. — М. : Вильямс, 2004. — 480 с.
7. Олифер В. Искусство оптимизации трафика / В. Олифер, Н. Олифер // Журнал сетевых решений LAN. — 2001. — № 12. — с. 21–26.
8. Rosen, E. Multiprotocol Label Switching Architecture / E. Rosen, A. Viswanathan, R. Callon. — RFC 3031, 2001. — 61 с.
9. Томас Т. Структура и реализация сетей на основе протокола OSPF. Руководство Cisco / Том Томас. — М. : Вильямс, 2004. — 816 с.
10. Вивек Олвейн. Структура и реализация современной технологии MPLS. Руководство Cisco = Advanced MPLS Design and Implementation. — М.: Вильямс, 2004. — 480 с. — ISBN 1-58705-020-X
11. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. — М.: КУДИЦ-ОБРАЗ, 2001. — 368 с.

12. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.:«Вильямс», 2002. — С. 432. — ISBN 0-13-016093-8